Refine Search

Search Results -

Terms	Documents
L19 and L18	20

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L20

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Sunday, November 13, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L20	L19 and l18	20	L20
L19	705/51,57,59;380/229,278,231,232.ccls.	2385	L19
L18	((encrypt$ near2 (decrypt$ adj key$)) with public$) and @ad<=19990327	154	L18
L17	((encrypt$ near3 (decrypt$ adj2 key$)) with public$) and @ad<=19990327	309	L17
L16	L15 and L10	8	L16
L15	L10 or L11 or L12 or L13 or L14	204	L15
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L14	(5103476 | 5592549 | 4932054 | 5047928 | 5337357 | 5724424 | 5909492 | 5005122 | 4961142 | 5710887 | 4891838 | 5794259 | 4937863 | 5757908 | 5050213 | 5014234 | 5845070 | 5940807 | 4529870 | 5113519 | 5897622 | 5553143 | 4977594 | 5758068 | 5339091 | 5159182 | 5023907 | 5758069 | 5146499 | 5247575 | 5390297 | 5805802 | 3790700 | 5260999 | 5778173 | 5255106 | 4953209 | 5010571 | 5291596 | 5918213 | 5708709 | 5898777 |	50	L14

Reviewed

4924378 | 5895454 | 4658093 | 5058164 | 5204897 | 5138712 | 5530752 | 5191193)![PN]

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR

L13	('6073124'| 'EP 715244A'| 'US 6073124A'| '5715403'| 'JP408263440A') [ABPN1,NRPN,PN,TBAN,WKU]	6	L13
L12	('6073124'| 'EP 715244A'| 'US 6073124A'| '5715403'| 'JP408263440A')[URPN]	140	L12
L11	6073124.pn. or 5715403.pn.	5	L11
L10	L9 or L8	8	L10
L9	((encrypt$ near3 (decrypt? adj2 key$)) with public$) and @ad<=19990327	8	L9
L8	((encrypt$ near3 (decrypt? adj2 key$)) with public$) and @pd<=19990327	2	L8
L7	((encrypt$ near5 (descript? adj3 key$)) with public$) and @pd<=19990327	0	L7
L6	((encrypt$ near5 (descript? adj3 key$)) with public$) and @ad<=19990327	0	L6
L5	((encrypt$ near3 (descript? adj2 key$)) with public$) and @ad<=19990327	0	L5
L4	((encrypt$ near3 (descript? adj2 key$)) with public$) and @pd<=19990327	0	L4

DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR

L3	L1 and (encrypt$ same (decrypt$ with key$))	1	L3
L2	L1 and (encrypt$ same (decrypt$ with key$) same public$)	1	L2
L1	6072874.pn.	1	L1

END OF SEARCH HISTORY

L20: Entry 19 of 20 File: USPT Feb 20, 1990

US-PAT-NO: 4903296
DOCUMENT-IDENTIFIER: US 4903296 A

TITLE: Implementing a shared higher level of privilege on personal computers for copy protection of software

DATE-ISSUED: February 20, 1990

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chandra; Akhileshwari N.	Mahopac	NY		
Comerford; Liam D.	Carmel	NY		
White; Steve R.	New York	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 06/930219 [PALM]
DATE FILED: November 12, 1986

PARENT-CASE:
This application is a division of U.S. Ser. No. 06/651,184 filed on Nov. 14, 1984, now U.S. Pat. No. 4,644,493.

INT-CL: [04] H04L 9/00

US-CL-ISSUED: 380/4; 364/969, 364/969.2, 364/969.4
US-CL-CURRENT: 705/56; 380/282, 705/57

FIELD-OF-SEARCH: 364/200, 364/900, 360/131, 380/3, 380/4, 380/49, 380/25

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4168396	September 1979	Best	364/900
☐	4246638	January 1981	Thomas	364/200
☐	4465901	August 1984	Best	364/200

☐	4558176	December 1985	Arnold et al.	364/900
☐	4573119	February 1986	Westheimer et al.	364/200
☐	4577289	March 1986	Comerford et al.	364/900

ART-UNIT: 237

PRIMARY-EXAMINER: Heckler; Thomas M.

ASSISTANT-EXAMINER: Mills; John G.

ATTY-AGENT-FIRM: Arnold; Jack M.

ABSTRACT:

Method and apparatus which restricts software, distributed on magnetic media, to use on a single computing machine. The original medium is functionally uncopyable, until it is modified by the execution of a program stored in a tamper proof co-processor which forms a part of the computing machine. The modified software on the original medium may then be copied, but the copy is operable only on the computing machine containing the co-processor that performed the modification.

4 Claims, 20 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 19 of 20 File: USPT Feb 20, 1990

DOCUMENT-IDENTIFIER: US 4903296 A
TITLE: Implementing a shared higher level of privilege on personal computers for copy protection of software

Application Filing Date (1):
19861112

Detailed Description Text (21):
3. The decryption key in encrypted form where the encryption is by the RSA public key provided by the support hardware manufacturer.

Current US Cross Reference Classification (2):
705/57

L20: Entry 19 of 20 File: USPT Feb 20, 1990

DOCUMENT-IDENTIFIER: US 4903296 A
TITLE: Implementing a shared higher level of privilege on personal computers for copy protection of software

Application Filing Date (1):
19861112

Detailed Description Text (21):
3. The decryption key in encrypted form where the encryption is by the RSA public key provided by the support hardware manufacturer.

Current US Cross Reference Classification (2):
705/57

L20: Entry 20 of 20 File: USPT Dec 10, 1985

US-PAT-NO: 4558176
DOCUMENT-IDENTIFIER: US 4558176 A

TITLE: Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software

DATE-ISSUED: December 10, 1985

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Arnold; Mark G.	Laramie	WY	82070	
Winkel; Mark D.	Loveland	CO	80537	

APPL-NO: 06/420562 [PALM]
DATE FILED: September 20, 1982

INT-CL: [04] H04K 9/00

US-CL-ISSUED: 178/22.08; 178/22.09, 364/900
US-CL-CURRENT: 713/190; 380/29, 705/51

FIELD-OF-SEARCH: 178/22.08, 178/22.09, 364/200, 364/300, 364/900, 340/825.34

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3958081	June 1976	Ehrsam et al.	364/200
☐	3996449	December 1976	Attanasio et al.	340/825.34
☐	4087856	May 1978	Attanasio	364/200
☐	4120030	October 1978	Johnstone	
☐	4168396	September 1979	Best	
☐	4183085	January 1980	Roberts et al.	364/200
☐	4193131	March 1980	Lennon et al.	
☐	4200770	April 1980	Hellman et al.	178/22.11
☐	4238854	December 1980	Ehrsam et al.	

☐	4246638	January 1981	Thomas	364/200
☐	4278837	July 1981	Best	
☐	4306289	December 1981	Lumley	364/200
☐	4319079	March 1982	Best	
☐	4446519	May 1984	Thomas	364/300
☐	4454594	June 1984	Heffron et al.	364/900
☐	4458315	July 1984	Uchenick	364/200
☐	4471163	September 1984	Donald et al.	364/200

OTHER PUBLICATIONS

Diffie et al., "Privacy & Authentication: An Introduction to Cryptography", IEEE Trans. Inform. Theory, Mar. 1979, pp. 397-427.
Kunheim, Alan, Cryptograph: A Primer, 1981, pp. 6-8, 285, 286, 294, 334, 335.

ART-UNIT: 221

PRIMARY-EXAMINER: Cangialosi; Salvatore

ASSISTANT-EXAMINER: Steinberger; Brian

ABSTRACT:

A method and apparatus are provided for inhibiting unauthorized copying, unauthorized usage and automated cracking of proprietary software used in computer systems. The computer systems execute protected programs, which are protected by encapsulation and/or encryption. To provide security against unauthorized copying of software, means are provided that detect and inhibit automated cracking of protected programs. These means will destroy or make inaccessible information in the CPU during conditions when automated cracking could occur. These means will also store interrupt contexts in secret to prevent implementation of automated cracking. Additional features may be provided to allow operation as a general purpose computer system, where protected programs are distributed using public key cryptography and a means is provided to convert from this distribution form to the protected execution form.

12 Claims, 13 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 20 of 20 File: USPT Dec 10, 1985

DOCUMENT-IDENTIFIER: US 4558176 A
TITLE: Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software

Application Filing Date (1):
19820920

Detailed Description Text (7):
In the preferred embodiment, the distribution format consists of two parts: a public key preamble, followed by the program encrypted using a large block cipher, such as DES. The software vendor will first select a DES key which will be used to encrypt the program. Then the vendor forms the public key preamble by encrypting the DES key using a public key algorithm with the public encryption key for the customer's computer. (Note that each computer will have a unique decryption key built into it and a corresponding encryption key that is made public.) This system provides good security while making distribution easy and permitting reasonable program load time.

Detailed Description Text (104):
When the user orders software, he sends the PUBRAN's public encryption key, the serial number, and manufacturer's digital signature number to the software vendor. The software vendor then checks the digital signature to determine if the user is using a software simulator or a bonafide PUBRAN unit made by the manufacturer. In the latter case, the software vendor will customize the software for the user's PUBRAN unit and then send it to the user. The format for secure program distribution consists of the body of the program which is encrypted in an address dependent large block cipher (e.g., a product cipher such as DES). This is preceded by a public key preamble containing the encryption/decryption key for the large block cipher. Standard media, such as floppy diskettes, are used for distribution.

Current US Cross Reference Classification (2):
705/51

L20: Entry 3 of 20 File: USPT Oct 22, 2002

US-PAT-NO: 6470085
DOCUMENT-IDENTIFIER: US 6470085 B1
**** See image for Certificate of Correction ****

TITLE: Application package and system for permitting a user to use distributed application package on the term of the use thereof

DATE-ISSUED: October 22, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Uranaka; Sachiko	Tokyo			JP
Kiyono; Masaki	Kamakura			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Matsushita Electric Industrial Co., Ltd.	Osaka			JP	03

APPL-NO: 08/915665 [PALM]
DATE FILED: August 21, 1997

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	8-286345	October 29, 1996

INT-CL: [07] H04 L 9/32

US-CL-ISSUED: 380/231
US-CL-CURRENT: 380/231

FIELD-OF-SEARCH: 380/202, 380/231, 705/51, 705/52, 705/56, 705/57, 705/58

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5319705	June 1994	Halter et al.	705/54
☐	5440631	August 1995	Akiyama et al.	705/53
☐	5857020	January 1999	Peterson, Jr.	705/52

☐	5907617	May 1999	Ronning	705/52

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
7-288519	October 1995	JP	
7-295674	November 1995	JP	
8-54951	February 1996	JP	

OTHER PUBLICATIONS

Schneier, Applied Cryptography, Oct. 1995, John Wiley and Sons, Inc., p. 368.*
Menezes et al. Handbook of Applied Cryptography, CRC Press, Oct. 17, 1996, p. 397.

ART-UNIT: 2131

PRIMARY-EXAMINER: Hayes; Gail

ASSISTANT-EXAMINER: Lathan; Bryan

ATTY-AGENT-FIRM: Gopstein; Israel Clark & Brody

ABSTRACT:

A system for permitting only an authentic user to play a desired application contained in a distributed application package in one of predetermined operation, e.g., free play mode, charged mode, limit-attached play mode, etc. The system comprises a client for playing an application under the control of a server connected with the client through a communication network. The application package (the volume) includes a distribution descriptor which contains mode codes assigned to the volume and the applications of the volume. The data of distribution descriptor is decided and stored in the descriptor at the time of distribution of the volume. This feature makes the system flexible. There is also disclosed a system operatable without communicating with a server.

42 Claims, 39 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 3 of 20 File: USPT Oct 22, 2002

DOCUMENT-IDENTIFIER: US 6470085 B1
** See image for Certificate of Correction **
TITLE: Application package and system for permitting a user to use distributed application package on the term of the use thereof

Application Filing Date (1):
19970821

Brief Summary Text (13):
For any type of charged information, charged information has been encrypted with a key and recorded on a DVD when obtained by a user. If distributed charged information to be played is of the limitlessly playable type, the charged information processing is achieved in the following way: the key is first obtained in a user public key-encrypted form from the DVD on which the key has been recorded at the time of selling the DVD; the user public key-encrypted key is decrypted with a user secret key stored in a IC card into a decrypted key; and the encrypted charged information is decrypted with the decrypted key and consumed (that is, played or executed). The user-public key-encrypted key may be obtained on line from the server serving the client (device).

Current US Original Classification (1):
380/231

L20: Entry 4 of 20 File: USPT Aug 6, 2002

US-PAT-NO: 6430292
DOCUMENT-IDENTIFIER: US 6430292 B1

TITLE: System and method for controlling disclosure time of information

DATE-ISSUED: August 6, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ito; Hiromichi	Yokohama			JP
Arai; Masato	Yokohama			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Hitachi, Ltd.	Tokyo			JP	03

APPL-NO: 09/110144 [PALM]
DATE FILED: July 6, 1998

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-181186	July 7, 1997

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 380/280; 380/277, 380/278, 380/279
US-CL-CURRENT: 380/280; 380/277, 380/278, 380/279

FIELD-OF-SEARCH: 380/277-280, 725/31, 705/51, 705/54

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5249230	September 1993	Mihm, Jr.	380/249
☐	5319705	June 1994	Halter et al.	705/54
☐	5392351	February 1995	Hasebe et al.	705/51
☐	5594794	January 1997	Eyer et al.	380/231
☐	5640453	June 1997	Schuchman et al.	380/211

☐	5706348	January 1998	Gray et al.	713/160
☐	5889861	March 1999	Ohashi et al.	380/247
☐	6029045	February 2000	Picco et al.	455/5.1
☐	6144401	November 2000	Casement et al.	725/93
☐	6157723	December 2000	Schultz	380/273

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
8102735	April 1996	JP	

OTHER PUBLICATIONS

E. Okamoto, Angio Riron Nyuumon, "An Introduction of the Theory of Cryptography", pp. 11-112, Kyoritsu Syuppan Kabushiki Kaisay, Feb. 25, 1993.

ART-UNIT: 2132

PRIMARY-EXAMINER: Decady; Albert

ASSISTANT-EXAMINER: Kabakoff; Steve

ATTY-AGENT-FIRM: Antonelli, Terry, Stout & Kraus, LLP

ABSTRACT:

A key managing system for implementing simultaneous disclosure of information. The invention includes an information transmitting apparatus which transmits a date and time at which secrecy protection of information is ended to a key controlling apparatus. The key controlling apparatus searches a key control table indicating a relation between decryption keys and decryption key disclosure dates & times for an encryption key that forms a pair in conjunction with a decryption key associated with the date & time transmitted by the information transmitting apparatus. The key controlling apparatus then transmits an encryption key found in the search to the information transmitting apparatus. The key controlling apparatus also discloses a decryption key for the present date & time to an information receiving apparatus in response to a request for a decryption key at a present date and time. The information transmitting apparatus, upon receipt of the encryption key, encrypts information by using the encryption key and then transmits the encrypted information to the information receiving apparatus. The date and time, at which secrecy protection of information is ended is appended to the encrypted information. The information receiving apparatus, upon the present date and time becoming coincident with the date and time appended to the received encrypted information, acquires a disclosed decryption key and decrypts the encrypted information by using the decryption key.

29 Claims, 15 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 4 of 20 File: USPT Aug 6, 2002

DOCUMENT-IDENTIFIER: US 6430292 B1
TITLE: System and method for controlling disclosure time of information

Application Filing Date (1):
19980706

Current US Cross Reference Classification (2):
380/278

CLAIMS:

12. A key controlling apparatus for controlling publicity of encryption and decryption keys used for encrypting and decrypting information respectively, said key controlling apparatus comprising: a key storage for storing at least a pair of said encryption and decryption keys for encrypting and decrypting information respectively; a key control table storage for storing a key control table indicating a relation between said decryption keys stored in said key storage and disclosure times of said decryption keys; a key searching means for searching said key control table stored in said key control table storage for a decryption key that can be disclosed at a current time specified by an information encrypting apparatus for encrypting information and an encryption key forming a pair corresponding to said decryption key; an encryption key transmitting means for transmitting an encryption key resulting from the search performed by said key searching means to said information encrypting apparatus; and a decryption key disclosing means for disclosing a decryption key, that can be disclosed at the current time according to said relation shown by said key control table stored in said key control table storage, to at least one of a plurality of information decrypting apparatuses each for decrypting information to permit said at least one information decrypting apparatus to decrypt encrypted data included in encrypted information having been previously acquired by said information decrypting apparatus, wherein said encrypted data is decrypted using said decryption key acquired at a disclosure time included in said encrypted information.

13. An information encrypting apparatus for encrypting information, comprising: encryption key acquiring means for acquiring an encryption key from a key controlling apparatus for controlling publicity of encryption and decryption keys by transmitting a time, at which secrecy protection of data to be encrypted will be ended, to said key controlling apparatus wherein said encryption key forms a pair corresponding to one of said decryption keys to be disclosed at a disclosure time in said key controlling apparatus; data encrypting means for encrypting data by using said encryption key acquired by said encryption key acquiring means; and encrypted information forming means for forming encrypted information to be transmitted to an information decrypting apparatus for decrypting information by adding data representing the time, at which secrecy protection of said encrypted data is to be ended, to said data encrypted by said data encrypting means.

L20: Entry 5 of 20 File: USPT Jul 9, 2002

US-PAT-NO: 6418421
DOCUMENT-IDENTIFIER: US 6418421 B1

TITLE: Multimedia player for an electronic content delivery system

DATE-ISSUED: July 9, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hurtado; Marco M.	Boca Raton	FL		
Gruse; George Gregory	Lighthouse Point	FL		
Downs; Edgar	Fort Lauderdale	FL		
Milsted; Kenneth Louis	Boynton Beach	FL		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/208774 [PALM]
DATE FILED: December 10, 1998

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This is a divisional of application Ser. No. 09/177,096, filed Oct. 22, 1998, which is a continuation-in-part of application Ser. No. 09/133,519, filed Aug. 13, 1998, now U.S. Pat. No. 6,226,618. The entire disclosure of prior application Ser. No. 09/177,096 is herein incorporated by reference. ATTORNEY APPLICATION TITLE OF THE DOC. NO. Ser. No. INVENTION INVENTOR (S) SE9-98-006 Secure Electronic Kenneth L. Milsted Content George Gregory Management Gruse Marco M. Hurtado Edgar Downs Cesar Medina SE9-98-007 Multimedia George Gregory Player Toolkit Gruse John J. Dorak, Jr. Kenneth L. Milsted SE9-98-008 Multimedia Kenneth L. Milsted Content Creation Qing Gong System Edgar Downs SE9-98-010 Key Management Jeffrey B. Lotspiech System for End- Marco M. Hurtado User Digital George Gregory Player Gruse Kenneth L. Milsted SE9-98-013 A method to Kenneth L. Milsted identify CD Craig Kindell content Qing Gong SE9-98-014 Toolkit for Richard Spagna delivering elec- Kenneth L. Milsted tronic content David P. Lybrand from an Online Edgar Downs store. SE9-98-015 A method and Kenneth L. Milsted apparatus to auto- Kha Kinh Nguyen matically create Qing Gong encode digital content SE9-98-016 A method and Kenneth L. Milsted apparatus to Qing Gong indicate an encoding rate for digital content

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/54; 705/51
US-CL-CURRENT: 705/54; 705/51

FIELD-OF-SEARCH: 380/4, 380/5, 380/281, 380/284, 705/51, 705/52, 705/53, 705/54, 705/57

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
WO 97/43717	November 1997	WO	
WO 98/13970	April 1998	WO	

ART-UNIT: 2132

PRIMARY-EXAMINER: Decady; Albert

ASSISTANT-EXAMINER: Smithers; Matthew

ATTY-AGENT-FIRM: Meyers; Steven J. Shofi; David M. Fleit, Kain, Gibbons, Gutman & Dongini P.L.

ABSTRACT:

A system for tracking usage of digital content on user devices. Electronic stores coupled to a network sell licenses to play digital content data to users. Content players, which receive from the network the licensed content data, are used to play the licensed content data. Additionally, a logging site that is coupled to the network tracks the playing of the content data. In particular, the logging site receives play information from the network, and the play information includes the number of times that the content data has been played by the associated content player. Also provided is a method for tracking usage of digital content on user devices. According to the method, a license to play digital content data is sold to a user, and the licensed content data is transmitted to a content player for the user. Further, information is transmitted to a logging site whenever the content data is played by the content player or copied from the content player to an external medium so that usage of the licensed content data can be tracked.

46 Claims, 21 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 5 of 20 File: USPT Jul 9, 2002

US-PAT-NO: 6418421
DOCUMENT-IDENTIFIER: US 6418421 B1

TITLE: Multimedia player for an electronic content delivery system

DATE-ISSUED: July 9, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hurtado; Marco M.	Boca Raton	FL		
Gruse; George Gregory	Lighthouse Point	FL		
Downs; Edgar	Fort Lauderdale	FL		
Milsted; Kenneth Louis	Boynton Beach	FL		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/208774 [PALM]
DATE FILED: December 10, 1998

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This is a divisional of application Ser. No. 09/177,096, filed Oct. 22, 1998, which is a continuation-in-part of application Ser. No. 09/133,519, filed Aug. 13, 1998, now U.S. Pat. No. 6,226,618. The entire disclosure of prior application Ser. No. 09/177,096 is herein incorporated by reference. ATTORNEY APPLICATION TITLE OF THE DOC. NO. Ser. No. INVENTION INVENTOR (S) SE9-98-006 Secure Electronic Kenneth L. Milsted Content George Gregory Management Gruse Marco M. Hurtado Edgar Downs Cesar Medina SE9-98-007 Multimedia George Gregory Player Toolkit Gruse John J. Dorak, Jr. Kenneth L. Milsted SE9-98-008 Multimedia Kenneth L. Milsted Content Creation Qing Gong System Edgar Downs SE9-98-010 Key Management Jeffrey B. Lotspiech System for End- Marco M. Hurtado User Digital George Gregory Player Gruse Kenneth L. Milsted SE9-98-013 A method to Kenneth L. Milsted identify CD Craig Kindell content Qing Gong SE9-98-014 Toolkit for Richard Spagna delivering elec- Kenneth L. Milsted tronic content David P. Lybrand from an Online Edgar Downs store. SE9-98-015 A method and Kenneth L. Milsted apparatus to auto- Kha Kinh Nguyen matically create Qing Gong encode digital content SE9-98-016 A method and Kenneth L. Milsted apparatus to Qing Gong indicate an encoding rate for digital content

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/54; 705/51
US-CL-CURRENT: 705/54; 705/51

FIELD-OF-SEARCH: 380/4, 380/5, 380/281, 380/284, 705/51, 705/52, 705/53, 705/54, 705/57

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
WO 97/43717	November 1997	WO	
WO 98/13970	April 1998	WO	

ART-UNIT: 2132

PRIMARY-EXAMINER: Decady; Albert

ASSISTANT-EXAMINER: Smithers; Matthew

ATTY-AGENT-FIRM: Meyers; Steven J. Shofi; David M. Fleit, Kain, Gibbons, Gutman & Dongini P.L.

ABSTRACT:

A system for tracking usage of digital content on user devices. Electronic stores coupled to a network sell licenses to play digital content data to users. Content players, which receive from the network the licensed content data, are used to play the licensed content data. Additionally, a logging site that is coupled to the network tracks the playing of the content data. In particular, the logging site receives play information from the network, and the play information includes the number of times that the content data has been played by the associated content player. Also provided is a method for tracking usage of digital content on user devices. According to the method, a license to play digital content data is sold to a user, and the licensed content data is transmitted to a content player for the user. Further, information is transmitted to a logging site whenever the content data is played by the content player or copied from the content player to an external medium so that usage of the licensed content data can be tracked.

46 Claims, 21 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 5 of 20 File: USPT Jul 9, 2002

DOCUMENT-IDENTIFIER: US 6418421 B1
TITLE: Multimedia player for an electronic content delivery system

Application Filing Date (1):
19981210

Brief Summary Text (18):
There is a need to overcome the above-mentioned drawbacks and to provide a multimedia player for an electronic content delivery system. One embodiment of the present invention provides a method of playing digital content data that has been compressed and encrypted with a first encrypting key on a system. According to the method, at least part of the content data is decrypted with a first decrypting key that corresponds to the first encrypting key. The decrypted content data is decompressed to produce decompressed content data, and the decompressed content data is played. In one preferred method, multiple segments of a second decrypting key that are stored separately on the system are retrieved, and the first decrypting key is decrypted using the second decrypting key. In such embodiments, the first decrypting key can be used to decrypt data that has been encrypted with the first encrypting key, and the second decrypting key can be used to decrypt data that has been encrypted with the second encrypting key. Further, in various embodiments, an encrypting key and its corresponding decrypting key can be symmetric keys (i.e., identical) or a key pair (e.g., a public key and its corresponding private key).

Current US Cross Reference Classification (1):
705/51

L20: Entry 6 of 20 File: USPT May 7, 2002

US-PAT-NO: 6385723
DOCUMENT-IDENTIFIER: US 6385723 B1
**** See image for Certificate of Correction ****

TITLE: Key transformation unit for an IC card

DATE-ISSUED: May 7, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Richards; Timothy Philip	Herts			GB

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Mondex International Limited				GB	03

APPL-NO: 09/075974 [PALM]
DATE FILED: May 11, 1998

PARENT-CASE:
PRIORITY APPLICATION This application claims priority to U.S. Provisional application No. 60/046,514 filed on May 15, 1997, and entitled "Design for a Multi Application Smart Card", which is hereby incorporated by reference.

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 713/160; 713/172, 380/278, 380/282, 380/285
US-CL-CURRENT: 713/160; 380/278, 380/282, 380/285, 713/172

FIELD-OF-SEARCH: 713/160, 713/172, 380/278-285

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4214230	July 1980	Fak et al.	
☐	4218582	August 1980	Hellman et al.	
☐	4259720	March 1981	Campbell	
☐	4302810	November 1981	Bouricius et al.	
☐	4305059	December 1981	Benton	

WO9320538	October 1993	WO
WO9321612	October 1993	WO
WO9619771	June 1996	WO
WO9628795	September 1996	WO
WO9638825	December 1996	WO
WO9843212	October 1998	WO
WO9910824	March 1999	WO
WO9916031	April 1999	WO

OTHER PUBLICATIONS

Schneier, "Applied Cryptography, 2nd Edition, "Chptr 3, Sec. 3.1, p. 51, 1996.*
Davies et al., "Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer," John Wiley & Sons 1984.

ART-UNIT: 2132

PRIMARY-EXAMINER: Decady; Albert

ASSISTANT-EXAMINER: Kabakoff; Steve

ATTY-AGENT-FIRM: Baker Botts L.L.P.

ABSTRACT:

A multi-application IC card system and method is disclosed providing a secure data transmission technique. The method is used, for example, to load an application from an application provider, which could be remote, to an IC card. At least a portion of the application is encrypted using a transfer key. The transfer key is then encrypted using the public key of a public/secret key pair of the intended IC card to form a key transformation unit. The encrypted application and key transformation unit are then sent to the IC card and the IC card decrypts the key transformation unit using its secret key. The transfer key is then recovered and used to decrypt the encrypted application. The application can then by stored on the IC card and accessed by the card user.

74 Claims, 11 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 6 of 20 File: USPT May 7, 2002

DOCUMENT-IDENTIFIER: US 6385723 B1
** See image for Certificate of Correction **
TITLE: Key transformation unit for an IC card

Application Filing Date (1):
19980511

Brief Summary Text (13):
In a preferred embodiment, the secure loading system and method allows the application provider to encrypt two or more portions of the application to be transmitted with two or more different keys, encrypt the two or more keys with the public key of the IC card to form a key transformation unit including the locations of the encrypted portions. Both the encrypted application and the key transformation unit are sent to the IC card. Because the decryption keys are encrypted with the IC card's public key, only the IC card's secret key can decrypt the key transformation unit. The transfer keys and the locations of the encrypted portions are recovered from the decrypted key transformation unit and the application is decrypted using the recovered transfer keys. This ensures that only the intended IC card can decrypt and use the application which was transmitted to that IC card.

Current US Cross Reference Classification (1):
380/278

L20: Entry 7 of 20 File: USPT May 1, 2001

US-PAT-NO: 6226618
DOCUMENT-IDENTIFIER: US 6226618 B1

TITLE: Electronic content delivery system

DATE-ISSUED: May 1, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Downs; Edgar	Fort Lauderdale	FL		
Gruse; George Gregory	Lighthouse Point	FL		
Hurtado; Marco M.	Boca Raton	FL		
Lehman; Christopher T.	Delray Beach	FL		
Milsted; Kenneth Louis	Boynton Beach	FL		
Lotspiech; Jeffrey B.	San Jose	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/133519 [PALM]
DATE FILED: August 13, 1998

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This non-provisional application claims subject matter that is technically related to the following applications that are commonly assigned herewith to International Business Machines (IBM). APPLI- CATION ATTORNEY SERIAL TITLE OF THE DOC. NO. NO. INVENTION INVENTOR(S) SE9-98-006 09/152,756 Secure Electronic Kenneth L. Milsted Content George Gregory Gruse Management Marco M. Hurtado Edgar Downs Cesar Medina SE9-98-007 09/209,440 Multimedia Player George Gregory Gruse Toolkit John J. Dorak, Jr. Kenneth L. Milsted SE9-98-008 09/241,276 Multimedia Content Kenneth L. Milsted Creation System Qing Gong Edgar Downs SE9-98-009 09/177,096 System for Tracking George Gregory Gruse End-User Electronic John J. Dorak, Jr. Content Kenneth L. Milsted SE9-98-010 09/203,307 Key Management Jeffrey B. Lotspiech System for End- Marco M. Hurtado User Digital Player George Gregory Gruse Kenneth L. Milsted SE9-98-011 09/208,774 Multi-media player Marco M. Hurtado for an Electronic George Gregory Gruse Content Delivery Edgar Downs System Kenneth L. Milsted SE9-98-013 09/203,306 A method to Kenneth L. Milsted identify CD content Craig Kindell Qing Gong SE9-98-014 09/203,315 Toolkit for Richard Spagna delivering electronic Kenneth L. Milsted content from an David P. Lybrand Online store. Edgar Downs SE9-98-015 09/201,622 A method and Kenneth L. Milsted apparatus to Kha Kinh Nguyen automatically create Qing Gong encode audio SE9-98-016 A method and Kenneth L. Milsted apparatus to Qing Gong indicate an encoding rate for audio

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 705/1; 705/1, 705/26, 705/27, 705/51, 705/53, 705/57, 705/59, 705/71, 380/4, 380/23, 380/24, 380/25, 380/44, 380/279, 380/281, 380/282
US-CL-CURRENT: 705/1; 380/279, 380/281, 380/282, 380/285, 380/30, 380/44, 705/26, 705/27, 705/51, 705/53, 705/57, 705/59 , 705/71

FIELD-OF-SEARCH: 705/4, 705/51, 705/53, 705/57, 705/59, 705/71, 705/26, 705/27, 380/4, 380/44, 380/23, 380/25, 380/281, 380/282, 380/279, 707/9

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4200770	April 1980	Hellman et al.	
☐	4218582	August 1980	Hellman et al.	
☐	4272810	June 1981	Gates et al.	
☐	4405829	September 1983	Rivest et al.	
☐	4424414	January 1984	Hellman et al.	
☐	4463387	July 1984	Hashimoto et al.	
☐	4528643	July 1985	Freeny, Jr.	
☐	4731840	March 1988	Mniszewski et al.	
☐	4757534	July 1988	Matyas et al.	
☐	4782529	November 1988	Shima	
☐	4803725	February 1989	Horne et al.	
☐	4809327	February 1989	Shima	
☐	4825306	April 1989	Robers	
☐	4868687	September 1989	Penn et al.	
☐	4868877	September 1989	Fischer	
☐	4878246	October 1989	Pastor et al.	
☐	4879747	November 1989	Leighton et al.	
☐	4905163	February 1990	Garber et al.	
☐	4926479	May 1990	Goldwasser et al.	
☐	4944006	July 1990	Citta et al.	
☐	4995082	February 1991	Schnorr	
☐	5005200	April 1991	Fischer	
☐	5130792	July 1992	Tindell et al.	
☐	5159634	October 1992	Reeds, III	
☐	5191573	March 1993	Hair	
☐	5214702	May 1993	Fischer	

☐				
☐	5915025	December 1999	Taguchi et al.	380/44
☐	5982892	November 1999	Hicks et al.	705/71
☐	5991399	November 1999	Graunke et al.	380/279
☐	5999629	December 1999	Heer et al.	705/51

OTHER PUBLICATIONS

J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, Feb., 1993, pp. 1-37.
S. Kent, "Privacy Enhancement or Internet Electronic Mail: Part II: Certificate-Based Key Management". RFC 1422, Feb., 1993, pp. 1-28.
D. Balenson, "Privace Enhancement for Internet Mail: Part III: Algorithms, Modes, and Indentifiers", RFC 1423, Feb. 1993, pp. 1-13.
B. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, Feb. 1993, pp. 1-8.

ART-UNIT: 274

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Nguyen; Nga B.

ATTY-AGENT-FIRM: Meyers; Steven J. Soucar; Steven J. Fleit, Kain, Gibbons, Gutman & Bongini P.L.

ABSTRACT:

Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using a second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

26 Claims, 20 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 7 of 20 File: USPT May 1, 2001

DOCUMENT-IDENTIFIER: US 6226618 B1
TITLE: Electronic content delivery system

Abstract Text (1):
Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using a second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

Application Filing Date (1):
19980813

Brief Summary Text (12):
Briefly, in accordance with the present invention, disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using ia second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

Current US Cross Reference Classification (9):
705/51

Current US Cross Reference Classification (11):
705/57

Current US Cross Reference Classification (12):
705/59

CLAIMS:

5. The method as defined in claim 4, wherein the step of transferring the decrypted first decrypting key includes the sub-steps of:

re-encrypting the first decrypting key using a third encrypting key, the third encrypting key being a public key of the user;

transferring the decrypted and re-encrypted first decrypting key to the user's system; and

decrypting the re-encrypted first decrypting key using a third decrypting key, the third decrypting key being a corresponding private key of the user.

11. A method of securely providing data to a user's system, the data being encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, said method comprising the steps of:

transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key;

decrypting the data decrypting key using the first private key;

re-encrypting the data decrypting key using a second public key;

transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and

decrypting the re-encrypted data decrypting key using the second private key.

17. A method of operating a clearinghouse to provide integrity in a channel of commerce that includes a provider, a distributor, and a purchaser, the provider producing data and encrypting the data so as to only be decryptable by a data decrypting key, the encrypted data being accessible to the purchaser, said method comprising the steps of:

encrypting the data decrypting key using a public key of the clearinghouse;

sending the encrypted data decrypting key from the provider to the distributor;

when the purchaser desires to purchase the data or a license to use the data, sending the encrypted data decrypting key from the distributor to the purchaser;

sending the encrypted data decrypting key from the purchaser to the clearing house;

decrypting the data decrypting key using a private key of the clearinghouse and re-encrypting the data decrypting key using a public key of the purchaser; and

sending the re-encrypted data decrypting key from the clearinghouse to the purchaser.

21. A system for securely providing data to a user's system, the system comprising:

a content system;

a first public key;

a first private key; which corresponds to the first public key;

a data encrypting key;

a data de-encrypting key for de-encrypting data encrypted using the data encrypting key;

first data encryption means for encrypting data so as to be decryptable only by a data decrypting key;

second data encryption means, using the first public key, for encrypting the decrypting key;

a clearing house;

first transferring means for transferring the data decrypting key which has been encrypted to the clearing house, wherein the clearinghouse possesses the first private key;

first decrypting means for decrypting the data decrypting key using the first private key;

a second public key;

a second private key; which corresponds to the second public key;

re-encryption means for re-encrypting the data decrypting key using the second public key;

second transferring means for transferring the re-encrypted data decrypting key to the user's system, wherein the user's system possesses the second private key; and

second decrypting means for decrypting the re-encrypted data decrypting key using the second private key.

Previous Doc Next Doc Go to Doc#

L20: Entry 8 of 20 File: USPT Sep 19, 2000

US-PAT-NO: 6122742
DOCUMENT-IDENTIFIER: US 6122742 A

TITLE: Auto-recoverable and auto-certifiable cryptosystem with unescrowed signing keys

DATE-ISSUED: September 19, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Young; Adam Lucas	New York	NY	10025	
Yung; Marcel Mordechay	New York	NY	10025	

APPL-NO: 08/878189 [PALM]
DATE FILED: June 18, 1997

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 713/201; 713/171, 713/176, 380/278, 380/281, 380/283
US-CL-CURRENT: 726/10; 380/278, 380/281, 380/283, 713/171, 713/176

FIELD-OF-SEARCH: 380/278, 380/281, 380/283, 380/44, 380/47, 380/28, 713/171, 713/176, 713/182, 713/201

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4200770	April 1980	Hellman et al.	
☐	4218582	August 1980	Hellman et al.	
☐	4405829	September 1983	Rivest et al.	
☐	4424414	January 1984	Hellman et al.	
☐	4625076	November 1986	Okamoto et al.	
☐	4641346	February 1987	Clark et al.	
☐	4748668	May 1988	Shamir et al.	
☐	4881264	November 1989	Merkle	
☐	4933970	June 1990	Shamir	
	4995082	February 1991	Schnorr	

☐			
☐	5005200	April 1991	Fischer
☐	5097504	March 1992	Camion et al.
☐	5231668	July 1993	Kravitz
☐	5276737	January 1994	Micali
☐	5315658	May 1994	Micali
☐	5557346	September 1996	Lipner et al.
☐	5557765	September 1996	Lipner et al.
☐	5633928	May 1997	Lenstra et al.
☐	5640454	June 1997	Lipner et al.
☐	5647000	July 1997	Leighton
☐	5796830	August 1998	Johnson et al.
☐	5815573	September 1998	Johnson et al.

OTHER PUBLICATIONS

"Applied Cryptography", Schneier, pp. 5, 28, 32, 42, 43, 178, 266, 421, 465, 597, 1995.
"Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes", Tatsuaki Okamoto, pp. 32-53. Federal Register/vol. 62, No.92/Tuesday, May 13,1997/Notices, pp. 26293,26294.
R. Anderson, M. Roe, "The GCHQ Protocol and Its Problems", Eurocrypt '97, pp. 134-148, Springer-Verlag 1997.
M. Bellare, P. Rogaway, "Optimal Asymmetric Encryption", Eurocrypt '94, pp. 92-111, Springer-Verlag, 1994.
D. Chaum, "Blind Signatures For Untraceable Payments".
D. Chaum, T.P. Pedersen, "Wallet Databases with Observers".
D. Denning, D. Branstad, "A Taxonomy for Key Escrow Encryption Systems", Communications of the ACM, v. 39, n. 3, , 1996.
A. De Santis, Y. Desmedt, Y. Frankel, M. Yung, "How to Share a Function Securrely", ACM STOC '94, pp. 522-533, 1994.
Y. Desmedt. Y. Frankel, "Threshold cryptosystems", CRYPTO '89, pp. 307-315, Springer-Verlag, 1989.
Y. Desmedt, "Securing Traceability of Ciphertexts--Towards a Secure Software Key Escrow System", eurocrypt '95, pp. 147-157, Springer-Verlag, 1995.
W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, 22, pp. 644-654, 1976.
T. ElGamal, "A Public Key Crptosystem and a Signature Scheme Based on Discrete Logarithms", CRYPTO '84, pp. 10-18, Springer-Verlag, 1985.
P. Feldman, "A Practical Scheme for Non-interactive Verifiable Secret Sharing", 28th annual FOCS, pp. 427-437, 1987.
A. Fiat, A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems", CRYPTO '86, pp. 186-194, Springer-Verlag, 1987.
Y. Frankel, M. Yung, "Escrow Encryption Systems Visited: Attacks, Analysis and Designs", CRYPTO '95, Springer-Verlag, 1995.
R. Ganesan, "How To Use Key Escrow", Communications of the ACM, v. 39, n.3, p. 33, 1996.
S. Goldwasser, S. Micali, R. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks", SIAM Journal on Computing, vol. 17, n. 2, 1988.
IBM, SecureWay, key recovery technology document, available at http://www.ibm.com/Security/html/wp-keyrec.html (downloaded May 25, 1997).

N. Jefferies, C. Mitchell, M. Walker, "A Proposed Architecture for Trusted Third Party Services", Cryptography: Policy and Algorithms, LNCS 1029, Springer, 1996.
J. Kilian, F. Leighton, "Fair Cryptosystems, Revisited", CRYPTO '95, pp. 208-221, Springer-Verlag, 1995.
L. Lacy, D. Mitchell, W. Schell, "CryptoLib: Cryptography in Software", AT&T Bell Labs, Crypto@research.att.com.
A. Lenstra, P. Winkler, Y. Yacobi, "A Key Escrow System with Warrant Bounds", CRYPTO '95, pp. 197-207, Springer-Verlag, 1995.
S. Micali, "Fair Public-Key Cryptosystems", CRYPTO '92, pp. 113-138, Springer-Verlag, 1992.
K. Nyberg, R. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem".
T.P. Pedersen, "A Threshold Cryptosystem without a Trusted Party".
E. Verheul, H. Tilborg, "Binding ElGamal: A Fraud-Detectable Alternative to Key-Escrow Proposals", Eurocrypt '97, pp. 119-133, Springer-Verlag, 1997.
S. Walker, J. Winston, "Principles for Use of Encryption and Key Recovery", available at http://www.tis.com/docs/products/recoverkey/recoverkey.html (downloaded May 25, 1997).
A. Young, M. Yung, "Kleptography: Using Cryptography Against Cryptography", Eurocrypt '97, pp. 62-74, Springer-Verlag, 1997.
"Digital Systems", CRC Handbook of Applied Cryptography, Ch 11, pp. 425-444.
"Digital Systems", CRC Handbook of Applied Cryptography, Ch 11, pp. 445-464.
"Digital Systems", CRC Handbook of Applied Crytography, Ch 11, pp. 465-481.

ART-UNIT: 277

PRIMARY-EXAMINER: Peeso; Thomas R.

ATTY-AGENT-FIRM: Schweitzer Cornman Gross & Bondell LLP

ABSTRACT:

A method is provided for an escrow cryptosystem combined with an unescrowed digital signature scheme that uses a single public key per user. This system is overhead-free, does not require a cryptographic tamper-proof hardware implementation (i.e., can be done in software), and is publicly verifiable. The system cannot be used subliminally to enable a shadow public key system. Namely, an unescrowed public key system that is publicly displayed in a covert fashion. The cryptosystem contains a key generation mechanism that outputs a key triplet, and a certificate of proof that the keys were generated according to the algorithm. The key triplet consists of a public key, a private decryption key, and a private signing key. Using the public key and the certificate, the triplet can be verified efficiently by anyone to have the following properties: (1) the private signing key is known to the user, and (2) the private decryption key is recoverable by the escrow authorities. The system assures that the escrow authorities are not able to forge signatures or get the private signing key. The system is designed so that its internals can be made publicly scrutinizable (e.g., it can be distributed in source code form).

20 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 8 of 20 File: USPT Sep 19, 2000

DOCUMENT-IDENTIFIER: US 6122742 A
TITLE: Auto-recoverable and auto-certifiable cryptosystem with unescrowed signing keys

Application Filing Date (1):
19970618

Brief Summary Text (18):
In the recovery process, the escrow authorities use the user's certificate of recoverability, which is obtained from the CA, as an input signal. The escrow authorities process the certificate of recoverability, and the corresponding user's private decryption key or data encrypted using the corresponding public key is the resulting output signal. The escrow authorities never get access to the users signature key and cannot forge his signature.

Current US Cross Reference Classification (1):
380/278

CLAIMS:

5. A method for public key cryptosystem including a subset of the operations of encryption, decryption, key exchange, signing, signature verification, and authentication, involving a public key function based on nested trapdoors functions.

L20: Entry 9 of 20 File: USPT Jul 18, 2000

US-PAT-NO: 6092201
DOCUMENT-IDENTIFIER: US 6092201 A

TITLE: Method and apparatus for extending secure communication operations via a shared list

DATE-ISSUED: July 18, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Turnbull; James Arthur	Kanata			CA
Curry; Ian H.	Kanata			CA
Van Oorschot; Paul C.	Ottawa			CA
Hillier; Stephen William	Ottawa			CA

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Entrust Technologies				CA	03

APPL-NO: 09/014185 [PALM]
DATE FILED: January 27, 1998

PARENT-CASE:
This patent application is a continuation in part of co-pending patent application entitled METHOD AND APPARATUS FOR CREATING COMMUNITIES OF TRUST IN A SECURE COMMUNICATION SYSTEM having Ser. No. of 08/957,612, and having a filing date of Oct. 24, 1997.

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 713/201; 713/155, 713/158, 713/168, 380/231, 380/241, 380/278
US-CL-CURRENT: 726/4; 380/231, 380/241, 380/278, 713/155, 713/158, 713/168

FIELD-OF-SEARCH: 380/231, 380/232, 380/241, 380/278, 380/277, 713/155, 713/158, 713/168, 713/182, 713/201

PRIOR-ART-DISCLOSED:

OTHER PUBLICATIONS

Schneier, "Applied Cryptography", pp. 35, 37, 185, 186, 1995.

ART-UNIT: 277

PRIMARY-EXAMINER: Peeso; Thomas R.

ATTY-AGENT-FIRM: Markison & Reckamp

ABSTRACT:

A method and apparatus for extending secure communication operations via shared lists is accomplished by creating a shared list in accordance with authorization parameters by one user and subsequently accessing the shared list via the authorization parameters by this and other users. To create the list, a user within the secured communication system determines whether it has been enabled, or authorized, to create a shared list. If so, the user identifies at least one other user to be added to the shared list. Having identified another user, the user creating the shared list verifies that the secure communication parameters (which includes a public key certificate of an end-user or of a certification authority) it has received regarding the another user is trustworthy. If the secure communication parameters are identified as trustworthy, the secure communication parameters of the another user are added to the shared list. To authenticate the shared list, the user creating the list digitally signs it. Once the shared list is created, other users, if authorized, may access the shared list to obtain certificates (e.g., encryption and/or signature verification certificates) of the users contained in the list.

29 Claims, 5 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 9 of 20 File: USPT Jul 18, 2000

DOCUMENT-IDENTIFIER: US 6092201 A
TITLE: Method and apparatus for extending secure communication operations via a shared list

Application Filing Date (1):
19980127

Detailed Description Text (6):
As an alternative to the certification authority 22 being a stand-alone computing device, it may be embodied in the same computing device as the server/manager 24. The server/manager 24 administers the day to day operations of the secured communications system 10. For example, the day to day operations of the certification authority and/or server/manager include, but are not limited to, enabling end-users as members of a secure communications system, generating key pairs, generating certificates (e.g. for encryption or digital signatures), revoking certificates or public keys of end-users or other authorities which have previously been issued certificates, and key recovery (e.g. allowing end-users to be restored with encryption/decryption keys which have been lost, for example, due a forgotten password). Typically, to function as a server/manager 24, a computing device will include secure management software. For example, the secure management software may be Entrust/Manager manufactured by Entrust Technologies, Limited.

Current US Cross Reference Classification (1):
380/231

Current US Cross Reference Classification (3):
380/278

L20: Entry 10 of 20 File: USPT Jun 6, 2000

US-PAT-NO: 6072874
DOCUMENT-IDENTIFIER: US 6072874 A

TITLE: Signing method and apparatus using the same

DATE-ISSUED: June 6, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Shin; Kil-Ho	Nakai-machi			JP
Kobayashi; Kenichi	Nakai-machi			JP
Aratani; Toru	Nakai-machi			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Fuji Xerox Co., Ltd.	Tokyo			JP	03

APPL-NO: 08/777047 [PALM]
DATE FILED: December 30, 1996

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	8-011568	January 26, 1996

INT-CL: [07] H04 N 7/167

US-CL-ISSUED: 380/231; 380/229, 380/232, 380/278
US-CL-CURRENT: 380/231; 380/229, 380/232, 380/278

FIELD-OF-SEARCH: 380/4, 380/23, 380/25, 380/231, 380/232, 380/229, 380/278

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5050213	September 1991	Shear	380/25
☐	5457746	October 1995	Dolphin	380/4
☐	5537473	July 1996	Saward	380/16
☐	5557679	September 1996	Julin et al.	380/23

☐	5727065	March 1998	Dillon	380/49
☐	5742677	April 1998	Pinder et al.	380/4
☐	5825876	October 1998	Peterson, Jr.	380/4
☐	5845281	December 1998	Benson et al.	707/9

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
4-334227	November 1992	JP	

ART-UNIT: 276

PRIMARY-EXAMINER: Hayes; Gail O.

ASSISTANT-EXAMINER: Song; Ho S.

ATTY-AGENT-FIRM: Oliff & Berridge, PLC

ABSTRACT:

The present invention provides a signing apparatus used for signing by a user on usage information of a source provided in a format made available by the use of key information. The apparatus includes a unit for generating the usage information which is to be signed, a unit for performing a first computation by utilizing the key information which has been encrypted and the usage information, a unit for performing a second computation by utilizing a user's private key and a result of the first computation. The apparatus further includes a unit for performing a third computation by utilizing a result of the second computation, and thereby generating the key information which has been decrypted and a result of the computation performed on the usage information by utilizing the user's private key. The apparatus further includes a unit for making the source available by utilizing the decrypted key information.

13 Claims, 4 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 10 of 20 File: USPT Jun 6, 2000

DOCUMENT-IDENTIFIER: US 6072874 A
TITLE: Signing method and apparatus using the same

Application Filing Date (1):
19961230

Brief Summary Text (6):
Japanese Patent Application Laid-Open No. Hei. 4-334227 (1992) discloses a method of forcing a user of charged broadcasting program to execute the digital signature on fee imposition information so that future denial of use of the charged program may be prevented. According to the invention of the Laid-Open publication, an encrypted program and a decryption key for decrypting the encrypted program are transmitted to a broadcasting program receiving decoder from the broadcasting station. The decoder receives the request for providing a program from the receiver, and notifies the receiver of the amount of the fee imposed on watching and listening to the program. If the amount of the fee is acceptable to the receiver, he/she executes digital signature with respect to the amount of the fee and returns it to the decoder. Then the decoder examines the returned digital signature of the amount of the fee to verify whether the signature is generated by a legitimate receiver. After legitimacy of the signature is verified, the decoder decrypts the requested program by the key obtained in advance, and provides the program to the receiver.

Current US Original Classification (1):
380/231

Current US Cross Reference Classification (1):
380/229

Current US Cross Reference Classification (2):
380/232

Current US Cross Reference Classification (3):
380/278

L20: Entry 11 of 20 File: USPT Feb 8, 2000

US-PAT-NO: 6023689
DOCUMENT-IDENTIFIER: US 6023689 A

TITLE: Method for secure communication in a telecommunications system

DATE-ISSUED: February 8, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herlin; Harry	Grapevine	TX		
Luo; Tie	Arlington	TX		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Nokia Mobile Phones Limited	Espoo			FI	03

APPL-NO: 09/250638 [PALM]
DATE FILED: February 16, 1999

PARENT-CASE:
This application is a continuation of U.S. application Ser. No. 08/796,613, filed Feb. 7, 1997, now U.S. Pat. No. 5,915,021.

INT-CL: [06] H04 L 9/08, H04 L 9/00, H04 L 9/30

US-CL-ISSUED: 705/67; 380/247, 380/30, 380/277, 380/278, 705/71, 713/171
US-CL-CURRENT: 705/67; 380/247, 380/277, 380/278, 380/30, 705/71, 713/171

FIELD-OF-SEARCH: 380/255, 380/259, 380/260, 380/270, 380/277, 380/278, 380/283, 380/284, 380/285, 380/28, 380/30, 380/347-250, 705/50, 705/64, 705/65, 705/67, 705/71, 713/150, 713/168, 713/171

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4956863	September 1990	Goss	380/30
☐	5222140	June 1993	Beller et al.	380/30
☐	5299263	March 1994	Beller et al.	380/30
☐	5406628	April 1995	Beller et al.	380/30

☐	5557346	September 1996	Lipner et al.	380/21
☐	5557678	September 1996	Ganesan	380/21
☐	5588061	December 1996	Ganesan et al.	380/30
☐	5761305	June 1998	Vanstone et al.	380/21
☐	5784463	July 1998	Chen et al.	380/21
☐	5915021	June 1999	Herlin et al.	380/21

ART-UNIT: 362

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Rivers; Brian T.

ABSTRACT:

A method for sending a secure message in a telecommunications system utilizing public encryption keys. All authentication parameters of each of the users, including each user's decryption key that is known only to the user, are used to verify, by public key methods, the identity of a user sending a communication to another user of the system. During the authentication process, an encryption key for use in communications between the two users may also be generated. The generated encryption key may be a private session key. Once the initial authentication is completed, the private session key can be used to perform encryption that is less computationally demanding than public key methods. In an embodiment of the invention, two communicating users may use the method to authenticate each other and generate an encryption key that is used to encrypt subsequent communications between the users. During the process of this embodiment, two encryption keys are generated. A first encryption key is used only in the authentication process, and a second encryption key is used in both the authentication process and as the key for encrypting subsequent communications. Use of two encryption keys requires that each of the two users apply its decryption key to complete the authentication and encryption key agreement process successfully.

4 Claims, 5 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 11 of 20 File: USPT Feb 8, 2000

DOCUMENT-IDENTIFIER: US 6023689 A
TITLE: Method for secure communication in a telecommunications system

Application Filing Date (1):
19990216

Current US Cross Reference Classification (3):
380/278

CLAIMS:

1. In a telecommunications system having a first and second transceiving device, wherein each of the first and second transceiving devices is assigned a decryption key and a public encryption key, and said second transceiving device is assigned identifying information, a method for providing secure communications, said method comprising the steps of:

selecting a first session key at the second transceiving device;

encrypting the first session key using the public encryption key of said first transceiving device to generate a first message in the second transceiving device;

transmitting the first message to the first transceiving device;

decrypting the first message, at the first transceiving device using the decryption key of the first transceiving device to generate said first session key;

encrypting the identifying information in said second transceiving device using said first session key to generate a second message;

transmitting said second message from the second transceiving device to the first transceiving device;

decrypting the second message at the first transceiving device using said first session key to generate the identifying information;

verifying the identity of the second transceiving device using the identifying information; and

in response to a positive verification in said step of verifying the identity of the second transceiving device:

selecting a second session key at said first transceiving device;

encrypting said second session key using the public encryption key of the second transceiving device to generate a third message in the first transceiving device;

transmitting said third message to the second transceiving device;

decrypting said third message, at the second transceiving device using the

decryption key of the second transceiving device to generate said second session key; and

using said second session key to encrypt subsequent communications between the first and second transceiving devices.

2. The method of claim 1, wherein said system is assigned a decryption key and a public encryption key, and wherein said method further comprises the steps of:

calculating and assigning a certificate for the second transceiving device by applying the decryption key of the system to a resultant value of a selected function, wherein the selected function has as inputs the public encryption key of the second transceiving device and the identifying information.

Previous Doc Next Doc Go to Doc#

L20: Entry 12 of 20 File: USPT Sep 21, 1999

US-PAT-NO: RE36310
DOCUMENT-IDENTIFIER: US RE36310 E

TITLE: Method of transferring data, between computer systems using electronic cards

DATE-ISSUED: September 21, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bjerrum; Jorgen	Oure			DK
Ottosen; Steen	Odense So			DK
Nielsen; Sven Kjaer	Albertslund			DK

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Kommunedata I/S	Copenhagen			DK	03

APPL-NO: 08/644286 [PALM]
DATE FILED: May 10, 1996

REISSUE-DATA:

US-PAT-NO	DATE-ISSUED	APPL-NO	DATE-FILED
05311595	19940510	772372	19900607

INT-CL: [06] H04 L 9/12

US-CL-ISSUED: 380/25; 380/23
US-CL-CURRENT: 713/168; 380/278, 713/170

FIELD-OF-SEARCH: 380/23, 380/25

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4176246	November 1979	Gaetzli	380/23
☐	4467139	August 1984	Mollier	380/23
☐	4549075	October 1985	Saada et al.	380/23
☐	4656474	April 1987	Mollier	380/23

☐	4677670	June 1987	Henderson, Jr.	380/25
☐	4807288	February 1989	Ugon et al.	380/23
☐	4823388	April 1989	Mitzutani et al.	380/23
☐	4882779	November 1989	Rahtgen	380/25
☐	4907272	March 1990	Hazard et al.	380/23
☐	4910773	March 1990	Hazard et al.	380/25
☐	4926480	May 1990	Chaum	380/23
☐	4935962	June 1990	Austin	380/25
☐	4974193	November 1990	Beutelspacher et al.	380/25
☐	4989244	January 1991	Naruse et al.	380/23

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
0114368	August 1984	EP	
0147716	July 1985	EP	
0194839	April 1986	EP	
0277247	August 1988	EP	
0285520	October 1988	EP	
0396894	November 1990	EP	
166541B1	March 1991	EP	
2526977	June 1988	FR	
3681797	March 1988	DE	
1399020	June 1975	GB	

OTHER PUBLICATIONS

"Smart Credit Cards: The answer to cashless shopping" IEEE Spectrum pp. 43-49, Feb. 1984.

ART-UNIT: 222

PRIMARY-EXAMINER: Cangialosi; Salvatore

ATTY-AGENT-FIRM: Merchant Gould Smith Edell Welter & Schmidt

ABSTRACT:

When transferring data, an electronic document or the like from a first computer system (100) to a second computer system (200) via a data transmission line (300), e.g. a public data transmission line, a first output and input station (122) comprising a first electronic card (124) and a second output and input station (222) comprising a second electronic card (224) are used. The data is transferred to the first electronic card (124) from the first computer system (100) via the first station (122) and is encrypted in the first electronic card (124), whereupon the data is output from the first electronic card (124) in encrypted form and transferred via the first station (122) to the first computer system (100) and

therefrom to the data transmission line (300). The data is received by the other computer system (200) in encrypted form and is transferred to the second electronic card (224) via the second station (222), whereupon the data is decrypted in the second electronic card (224) and is output from the second electronic card via the second station (222) to the second computer system (200). As the data transfer between the first and the second computer system is carried out between the first and the second electronic card, no third parties have neither authorized or unauthorized possibility of interfering with the data transmission and possibly changing the data or the electronic document. The first and second electronic card (124, 224) constitute a coherent set of cards comprising coherent encryption/decryption keys input into the internal storages of the cards.

33 Claims, 6 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 12 of 20 File: USPT Sep 21, 1999

US-PAT-NO: RE36310
DOCUMENT-IDENTIFIER: US RE36310 E

TITLE: Method of transferring data, between computer systems using electronic cards

DATE-ISSUED: September 21, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bjerrum; Jorgen	Oure			DK
Ottosen; Steen	Odense So			DK
Nielsen; Sven Kjaer	Albertslund			DK

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Kommunedata I/S	Copenhagen			DK	03

APPL-NO: 08/644286 [PALM]
DATE FILED: May 10, 1996

REISSUE-DATA:

US-PAT-NO	DATE-ISSUED	APPL-NO	DATE-FILED
05311595	19940510	772372	19900607

INT-CL: [06] H04 L 9/12

US-CL-ISSUED: 380/25; 380/23
US-CL-CURRENT: 713/168; 380/278, 713/170

FIELD-OF-SEARCH: 380/23, 380/25

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4176246	November 1979	Gaetzli	380/23
☐	4467139	August 1984	Mollier	380/23
☐	4549075	October 1985	Saada et al.	380/23
☐	4656474	April 1987	Mollier	380/23

☐	4677670	June 1987	Henderson, Jr.	380/25
☐	4807288	February 1989	Ugon et al.	380/23
☐	4823388	April 1989	Mitzutani et al.	380/23
☐	4882779	November 1989	Rahtgen	380/25
☐	4907272	March 1990	Hazard et al.	380/23
☐	4910773	March 1990	Hazard et al.	380/25
☐	4926480	May 1990	Chaum	380/23
☐	4935962	June 1990	Austin	380/25
☐	4974193	November 1990	Beutelspacher et al.	380/25
☐	4989244	January 1991	Naruse et al.	380/23

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
0114368	August 1984	EP	
0147716	July 1985	EP	
0194839	April 1986	EP	
0277247	August 1988	EP	
0285520	October 1988	EP	
0396894	November 1990	EP	
166541B1	March 1991	EP	
2526977	June 1988	FR	
3681797	March 1988	DE	
1399020	June 1975	GB	

OTHER PUBLICATIONS

"Smart Credit Cards: The answer to cashless shopping" IEEE Spectrum pp. 43-49, Feb. 1984.

ART-UNIT: 222

PRIMARY-EXAMINER: Cangialosi; Salvatore

ATTY-AGENT-FIRM: Merchant Gould Smith Edell Welter & Schmidt

ABSTRACT:

When transferring data, an electronic document or the like from a first computer system (100) to a second computer system (200) via a data transmission line (300), e.g. a public data transmission line, a first output and input station (122) comprising a first electronic card (124) and a second output and input station (222) comprising a second electronic card (224) are used. The data is transferred to the first electronic card (124) from the first computer system (100) via the first station (122) and is encrypted in the first electronic card (124), whereupon the data is output from the first electronic card (124) in encrypted form and transferred via the first station (122) to the first computer system (100) and

therefrom to the data transmission line (300). The data is received by the other computer system (200) in encrypted form and is transferred to the second electronic card (224) via the second station (222), whereupon the data is decrypted in the second electronic card (224) and is output from the second electronic card via the second station (222) to the second computer system (200). As the data transfer between the first and the second computer system is carried out between the first and the second electronic card, no third parties have neither authorized or unauthorized possibility of interfering with the data transmission and possibly changing the data or the electronic document. The first and second electronic card (124, 224) constitute a coherent set of cards comprising coherent encryption/decryption keys input into the internal storages of the cards.

33 Claims, 6 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 12 of 20 File: USPT Sep 21, 1999

DOCUMENT-IDENTIFIER: US RE36310 E
TITLE: Method of transferring data, between computer systems using electronic cards

Application Filing Date (1):
19960510

Brief Summary Text (81):
The present invention furthermore relates to a system for transferring data, an electronic document or the like from a first computer system to a second computer system, said second computer system being autonomous in relation to said first computer system, via a data transmission line, e.g. a public data transmission line, in accordance with the method according to the first aspect of the invention, which system in accordance with the invention is characterized in that it comprises the first station and the second station, which are connected to and communicate with the first and the second computer system, respectively, and which furthermore via the first and the second computer system, respectively, and the corresponding interfacing means are connected to the data transmission line, as well as the first and the second electronic card, which constitute a coherent set of cards comprising the coherent encryption/decryption keys input into the internal storages of the cards. The coherent set of cards used in this system according to the invention preferably comprises cards of the type DES Smart Card (Philips), Super Smart Card (Bull) or CP8 Smart Card (Bull) or at least a card implemented on a printed circuit card, a thick-film substrate, a thin-film module, etc.

Brief Summary Text (82):
The present invention furthermore relates to a system for transferring data, an electronic document or the like from a first computer system to a second computer system, said second computer system being autonomous relative to said first computer system, via a data transmission line, e.g. a public data transmission line, said system being characterized in that it comprises said first station and said second station, which are connected to and communicate with said first and said second computer system, respectively, and which furthermore via said first and said second computer system, respectively, and corresponding interfacing means are connected to said data transmission line, as well as said first and said second card, which constitute a coherent set of cards comprising said coherent data input into said cards concerning said coherent encryption/decryption keys stored in said internal storages of said corresponding stations. The coherent set of data, which is used according to the system and the method according to the second aspect of the invention can be a magnetic card as well as an electronic card which again can be of above-mentioned type. In accordance with this aspect of the invention, any other medium can furthermore be used.

Current US Cross Reference Classification (1):
380/278

L20: Entry 13 of 20 File: USPT Sep 14, 1999

US-PAT-NO: 5953419
DOCUMENT-IDENTIFIER: US 5953419 A
**** See image for Certificate of Correction ****

TITLE: Cryptographic file labeling system for supporting secured access by multiple users

DATE-ISSUED: September 14, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Lohstroh; Shawn R.	Princeton	NJ		
McDonnal; William D.	Tigard	OR		
Grawrock; David	Aloha	OR		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Symantec Corporation	Cupertino	CA			02

APPL-NO: 08/642217 [PALM]
DATE FILED: May 6, 1996

INT-CL: [06] H04 L 9/02

US-CL-ISSUED: 380/21
US-CL-CURRENT: 713/165; 380/278

FIELD-OF-SEARCH: 380/21, 380/49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4854616	August 1989	Pond et al.	380/25
☐	4881263	November 1989	Herbison et al.	380/21
☐	5029207	July 1991	Gammie	380/10
☐	5052040	September 1991	Preston et al.	380/4
☐	5151938	September 1992	Griffin, III et al.	380/43
☐	5465299	November 1995	Matsumoto et al.	380/23

☐	5495533	February 1996	Linehan et al.	380/21
☐	5563946	October 1996	Cooper et al.	380/4
☐	5604803	February 1997	Aziz	380/25
☐	5615264	March 1997	Kazmierczak	380/4

ART-UNIT: 276

PRIMARY-EXAMINER: Hayes; Gail O.

ASSISTANT-EXAMINER: White; Carmen

ATTY-AGENT-FIRM: Fliesler, Dubb, Meyer & Lovejoy

ABSTRACT:

A system is disclosed for automatically distributing secured versions (*Sys.sub.-- D.sub.-- key*) of a file decryption key (Sys.sub.-- D.sub.-- key) to a plurality of file users by way of the file's security label. The label is defined to contain a plurality of Access-Control-Entries Records (ACER's) where each ACER includes a respective secured version (*Sys.sub.-- D.sub.-- key*) of the file decryption key. Each such secured version (*Sys.sub.-- D.sub.-- key*) is decipherable by a respective ACER private key. Each ACER may include respective other data such as:

(a) ACER-unique identifying data for uniquely identifying the ACER or an associated user;

(b) decryption algorithm identifying data for identifying the decryption process to be used to decrypt the encrypted *DATA* portion of the file; and

(c) special handling code for specifying special handling for the code-containing ACER. The label is preferably covered by a digital signature but includes an extension buffer that is not covered by the digital signature. Users who wish to have an ACER of their own added to the label may submit add-on requests by writing to the extension buffer.

53 Claims, 10 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 13 of 20 File: USPT Sep 14, 1999

DOCUMENT-IDENTIFIER: US 5953419 A
** See image for Certificate of Correction **
TITLE: Cryptographic file labeling system for supporting secured access by multiple users

Application Filing Date (1):
19960506

Current US Cross Reference Classification (1):
380/278

CLAIMS:

44. A method for distributing encrypted *FILE DATA* signals to a plurality of users and for providing respective authorized users among said plurality of users each with intelligible access to information represented by a plaintext version of the encrypted *FILE DATA* signals,

wherein said *FILE DATA* signals are producible by using a first encrypting algorithm in combination with a first encryption key to encrypt the plaintext version of said *FILE DATA* signals,

said method comprising the steps of:

(a) conveying the encrypted *FILE DATA* signals to a first data conveyance means;

(b) defining a companion first decryption algorithm and a companion first decryption key that are usable for decrypting the conveyed *FILE DATA* signals;

(c) for each respective authorized user, encrypting the companion first decryption key by using a respective second encryption algorithm in combination with a respective second encryption key to thereby produce a respective encrypted version of the companion first decryption key, wherein said second encryption key is a public key of the respective authorized user, and said respective second encryption algorithm is an asymmetric algorithm based on paired public and private keys;

(d) for each respective authorized user, conveying the respective encrypted version to the first conveyance means; and

(e) for each respective authorized user, associating at least partially by means of the first conveyance means, the respective encrypted version of the companion first decryption key with the conveyed *FILE DATA* signals.

L20: Entry 14 of 20 File: USPT Jun 29, 1999

US-PAT-NO: 5917910
DOCUMENT-IDENTIFIER: US 5917910 A

TITLE: Encrypting method and apparatus, recording method, decrypting method and apparatus, and recording medium

DATE-ISSUED: June 29, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ishiguro; Ryuji	Tokyo			JP
Minami; Masafumi	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sony Corporation	Tokyo			JP	03

APPL-NO: 08/721310 [PALM]
DATE FILED: October 15, 1996

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	7-267252	October 16, 1995

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/4; 380/44, 380/5, 380/46
US-CL-CURRENT: 705/57; 380/201, 380/44, 380/46

FIELD-OF-SEARCH: 380/3, 380/4, 380/5, 380/9, 380/21, 380/49, 380/44, 380/46

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5148422	September 1992	Sako et al.	369/44.26
☐	5327563	July 1994	Singh	380/4
☐	5412718	May 1995	Narasimhalu et al	380/4
☐	5416840	May 1995	Cane et al.	380/4

☐	5467398	November 1995	Pierce et al.	380/44
☐	5538773	July 1996	Kondo	428/64.1
☐	5563947	October 1996	Kikinis	380/4
☐	5572507	November 1996	Ozaki et al.	369/275.4
☐	5590200	December 1996	Nachman et al.	380/46
☐	5694469	December 1997	Le Rue	380/4

ART-UNIT: 276

PRIMARY-EXAMINER: Gregory; Bernarr E.

ASSISTANT-EXAMINER: Laufer; Pinchus M.

ATTY-AGENT-FIRM: Frommer Lawrence & Haug, LLP. Frommer; William S.

ABSTRACT:

When information to be recorded is encrypted by using an encryption key, an encryption key based on inherent information inherent in a recording medium is generated. The information to be recorded on the recording medium is encrypted based on the encryption key. The inherent information inherent in the recording medium is a specific information on a disk. When an encrypted information recorded on a recording medium is decrypted, there are reproduced from a recording medium a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of the encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of the random data to be inserted into a predetermined portion of the encrypted information. The random data is detected from the encrypted information stored the reproduced first file based on the data stored in the reproduced second file and indicating the predetermined portion of the random data. A decryption key is generated from the detected random data. The encrypted information of the reproduced first file is decrypted by using the decryption key.

19 Claims, 15 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 14 of 20 File: USPT Jun 29, 1999

DOCUMENT-IDENTIFIER: US 5917910 A
TITLE: Encrypting method and apparatus, recording method, decrypting method and apparatus, and recording medium

Application Filing Date (1):
19961015

Brief Summary Text (6):
A cryptosystem employing a key (an encryption key) includes two cryptosystems; a common-key cryptographic scheme and a public-key cryptosystem. In the common-key cryptosystem, a key (encryption key) used upon encryption is the same as a key (decryption key) used upon decryption. For example, of the common-key cryptosystems, a data encryption standard (DES) system is frequently employed. On the other hand, in the public-key cryptosystem, an encryption key and a decryption key are different from each other. In this public-key cryptosystem, the encryption key is opened to the public, but the decryption key is kept secret. In general, such encryption method and decryption method are known.

Current US Original Classification (1):
705/57

L20: Entry 15 of 20 File: USPT Jun 22, 1999

US-PAT-NO: 5915025
DOCUMENT-IDENTIFIER: US 5915025 A

TITLE: Data processing apparatus with software protecting functions

DATE-ISSUED: June 22, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Taguchi; Masahiro	Nakai-machi			JP
Kawano; Kenji	Nakai-machi			JP
Saito; Kazuo	Nakai-machi			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Fuji Xerox Co., Ltd.	Tokyo			JP	03

APPL-NO: 08/779643 [PALM]
DATE FILED: January 15, 1997

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	8-005559	January 17, 1996
JP	8-165637	June 26, 1996

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/44; 380/4, 380/9, 380/21, 380/46, 380/49, 380/50, 395/186
US-CL-CURRENT: 380/44; 380/46, 705/51

FIELD-OF-SEARCH: 380/4, 380/9, 380/21, 380/28, 380/44, 380/45, 380/46, 380/47, 380/49, 380/250, 395/186, 395/187.01

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4593384	June 1986	Kleijne	
☐	4747139	May 1988	Taaffe	380/44

☐	5337357	August 1994	Chou et al.	380/4
☐	5757907	May 1998	Cooper et al.	380/4

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
A-63-124153	May 1988	JP	
A-2-44447	February 1990	JP	
A-2-155034	June 1990	JP	
A-4-102920	April 1992	JP	

ART-UNIT: 276

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Oliff & Berridge, PLC

ABSTRACT:

A data processing apparatus with software protecting functions capable of enhancing the level of encryption security independently of the memory management method of the system comprising the apparatus. Upon receiving target data to be encrypted, an encryption key generation unit generates an encryption key in accordance with an attribute of the target data. Using the encryption key, an encryption unit encrypts the target data. The encrypted data is placed into a storage unit. When a request is made to process the encrypted data, a decryption key generation unit generates a decryption key in accordance with the attribute of the encrypted data. A decryption unit decrypts the encrypted data using the decryption key. The decrypted data is processed by a processing unit. A control unit supplies the encryption unit with the data processed by the processing unit as data to be encrypted.

19 Claims, 52 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 15 of 20 File: USPT Jun 22, 1999

DOCUMENT-IDENTIFIER: US 5915025 A
TITLE: Data processing apparatus with software protecting functions

Application Filing Date (1):
19970115

Detailed Description Text (12):
In the above constitution, data is initially encrypted and supplied from software suppliers to users over the network or by means of CO-ROM's and the like. The encryption method used in such cases is any one of well-known encryption methods offering high levels of encryption security. Illustratively, a software supplier may encrypt data for a user by utilizing the DES (Data Encryption Standard, the encryption algorithm disclosed in 1977 by the Standards Bureau, U.S. Department of Commerce, currently the American National Standards Institute). The encrypted data may be offered to the user together with a decryption key that is encrypted illustratively by a public key based on the RSA (Rivest, Shamir, Adleman; the algorithm devised by Ronald Rivest, Adi Shamir and Leonard Adleman) for a data processing apparatus with software protecting functions. The user transfers the encrypted data and the decryption key encrypted by the public key for the data processing apparatus, from the I/O interface 42 to the distributed software decryption means 32 for decryption. The distributed software decryption means 32 decrypts the decryption key by its own RSA secret Key, and subsequently decrypts the encrypted data by the decryption key. The data thus decrypted is sent directly to the encryption means 33 so as to be encrypted by a secret encryption method or encryption key. The user cannot access the decrypted data. The data encrypted by the encryption means 33 is stored into the storage means 41. The data processing means 31 causes the decryption means 34 to decrypt the encrypted data from the storage means 41, receives the decrypted data, and executes instructions included in the data. If any part of the data output by the data processing means 31 needs to be encrypted, that data part is encrypted by the encryption means 33 before being placed into the storage means 41.

Detailed Description Text (17):
In the constitution above, the encrypted data and decryption key are supplied over the network or by means of a CD-ROM and the like from a software supplier to the user. To load the encrypted data into the apparatus for execution requires initially that the decryption key encrypted by a public key for the apparatus be sent to the distributed software decryption means 52 via the I/O interface 62. The decrypted data is forwarded directly to the encryption means 53. At the same time, the key selection means 55 selects an encryption key group corresponding to the storage destination page number of the data. The selected encryption key group is fed from the key supply means 56 to the encryption means 53. The data sent to the encryption means 53 is encrypted by the key group supplied by the key supply means 56. Because the encryption method or encryption keys in this case are of secret nature, the user cannot access the decrypted data. The data encrypted by the encryption means 53 using a different encryption key group for each page is placed into the storage means 61. The excess pages not accommodated by the storage means 61 are swapped out to the hard disk 66. Where the data processing means 51 is to execute an encrypted program in the storage means 61, the key selection means 55 first selects from the key supply means 56 a decryption key group corresponding to

the data storage destination page. The decryption means 54 then decrypts the data using the selected decryption key group. The program thus decrypted is executed by the data processing means 51. If any part of the data output by the data processing means 51 needs to be encrypted, that data part is encrypted by the encryption means 53 before being placed into the storage means 61.

Current US Cross Reference Classification (2):
705/51

Previous Doc Next Doc Go to Doc#

Hit List

First Hit | Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 10 of 20 returned.

☐ 1. Document ID: US 6910020 B2

Using default format because multiple data bases are involved.

L20: Entry 1 of 20 File: USPT Jun 21, 2005

US-PAT-NO: 6910020
DOCUMENT-IDENTIFIER: US 6910020 B2

TITLE: Apparatus and method for granting access to network-based services based upon existing bank account information

DATE-ISSUED: June 21, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Oyama; Shuji	Kawasaki			JP
Sato; Akira	Kawasaki			JP

US-CL-CURRENT: 705/38; 380/228, 380/232, 705/50, 705/71, 705/76, 726/10

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 2. Document ID: US 6530020 B1

L20: Entry 2 of 20 File: USPT Mar 4, 2003

US-PAT-NO: 6530020
DOCUMENT-IDENTIFIER: US 6530020 B1
** See image for Certificate of Correction **

TITLE: Group oriented public key encryption and key management system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 3. Document ID: US 6470085 B1

L20: Entry 3 of 20 File: USPT Oct 22, 2002

US-PAT-NO: 6470085
DOCUMENT-IDENTIFIER: US 6470085 B1
** See image for Certificate of Correction **

TITLE: Application package and system for permitting a user to use distributed application package on the term of the use thereof

☐ 4. Document ID: US 6430292 B1

L20: Entry 4 of 20 File: USPT Aug 6, 2002

US-PAT-NO: 6430292
DOCUMENT-IDENTIFIER: US 6430292 B1

TITLE: System and method for controlling disclosure time of information

☐ 5. Document ID: US 6418421 B1

L20: Entry 5 of 20 File: USPT Jul 9, 2002

US-PAT-NO: 6418421
DOCUMENT-IDENTIFIER: US 6418421 B1

TITLE: Multimedia player for an electronic content delivery system

☐ 6. Document ID: US 6385723 B1

L20: Entry 6 of 20 File: USPT May 7, 2002

US-PAT-NO: 6385723
DOCUMENT-IDENTIFIER: US 6385723 B1
**** See image for Certificate of Correction ****

TITLE: Key transformation unit for an IC card

☐ 7. Document ID: US 6226618 B1

L20: Entry 7 of 20 File: USPT May 1, 2001

US-PAT-NO: 6226618
DOCUMENT-IDENTIFIER: US 6226618 B1

TITLE: Electronic content delivery system

☐ 8. Document ID: US 6122742 A

L20: Entry 8 of 20 File: USPT Sep 19, 2000

US-PAT-NO: 6122742
DOCUMENT-IDENTIFIER: US 6122742 A

TITLE: Auto-recoverable and auto-certifiable cryptosystem with unescrowed signing keys

☐ 9. Document ID: US 6092201 A

L20: Entry 9 of 20 File: USPT Jul 18, 2000

US-PAT-NO: 6092201
DOCUMENT-IDENTIFIER: US 6092201 A

TITLE: Method and apparatus for extending secure communication operations via a shared list

☐ 10. Document ID: US 6072874 A

L20: Entry 10 of 20 File: USPT Jun 6, 2000

US-PAT-NO: 6072874
DOCUMENT-IDENTIFIER: US 6072874 A

TITLE: Signing method and apparatus using the same

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L19 and L18	20

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Hit List

First Hit | Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 11 through 20 of 20 returned.

☐ 11. Document ID: US 6023689 A

Using default format because multiple data bases are involved.

L20: Entry 11 of 20 File: USPT Feb 8, 2000

US-PAT-NO: 6023689
DOCUMENT-IDENTIFIER: US 6023689 A

TITLE: Method for secure communication in a telecommunications system

DATE-ISSUED: February 8, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herlin; Harry	Grapevine	TX		
Luo; Tie	Arlington	TX		

US-CL-CURRENT: 705/67; 380/247, 380/277, 380/278, 380/30, 705/71, 713/171

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 12. Document ID: US RE36310 E

L20: Entry 12 of 20 File: USPT Sep 21, 1999

US-PAT-NO: RE36310
DOCUMENT-IDENTIFIER: US RE36310 E

TITLE: Method of transferring data, between computer systems using electronic cards

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 13. Document ID: US 5953419 A

L20: Entry 13 of 20 File: USPT Sep 14, 1999

US-PAT-NO: 5953419
DOCUMENT-IDENTIFIER: US 5953419 A
** See image for Certificate of Correction **

TITLE: Cryptographic file labeling system for supporting secured access by multiple

users

☐ 14. Document ID: US 5917910 A

L20: Entry 14 of 20 File: USPT Jun 29, 1999

US-PAT-NO: 5917910
DOCUMENT-IDENTIFIER: US 5917910 A

TITLE: Encrypting method and apparatus, recording method, decrypting method and apparatus, and recording medium

☐ 15. Document ID: US 5915025 A

L20: Entry 15 of 20 File: USPT Jun 22, 1999

US-PAT-NO: 5915025
DOCUMENT-IDENTIFIER: US 5915025 A

TITLE: Data processing apparatus with software protecting functions

☐ 16. Document ID: US 5812664 A

L20: Entry 16 of 20 File: USPT Sep 22, 1998

US-PAT-NO: 5812664
DOCUMENT-IDENTIFIER: US 5812664 A

TITLE: Key distribution system

☐ 17. Document ID: US 5586186 A

L20: Entry 17 of 20 File: USPT Dec 17, 1996

US-PAT-NO: 5586186
DOCUMENT-IDENTIFIER: US 5586186 A

TITLE: Method and system for controlling unauthorized access to information distributed to users

☐ 18. Document ID: US 5159633 A

L20: Entry 18 of 20 File: USPT Oct 27, 1992

US-PAT-NO: 5159633
DOCUMENT-IDENTIFIER: US 5159633 A
**** See image for Certificate of Correction ****

TITLE: Multimedia network system

☐ 19. Document ID: US 4903296 A

L20: Entry 19 of 20 File: USPT Feb 20, 1990

US-PAT-NO: 4903296
DOCUMENT-IDENTIFIER: US 4903296 A

TITLE: Implementing a shared higher level of privilege on personal computers for copy protection of software

☐ 20. Document ID: US 4558176 A

L20: Entry 20 of 20 File: USPT Dec 10, 1985

US-PAT-NO: 4558176
DOCUMENT-IDENTIFIER: US 4558176 A

TITLE: Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L19 and L18	20

Display Format: - Change Format

Previous Page Next Page Go to Doc#

L20: Entry 16 of 20 File: USPT Sep 22, 1998

US-PAT-NO: 5812664
DOCUMENT-IDENTIFIER: US 5812664 A

TITLE: Key distribution system

DATE-ISSUED: September 22, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bernobich; Elizabeth	New Haven	CT		
Heiden; Richard W.	Huntington	CT		
Sisson; Robert W.	Shelton	CT		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Pitney Bowes Inc.	Stamford	CT			02

APPL-NO: 08/708284 [PALM]
DATE FILED: September 6, 1996

INT-CL: [06] H04 L 9/08, H04 L 9/00, H04 L 9/30

US-CL-ISSUED: 380/21; 380/49, 380/50, 380/51, 380/54, 380/30, 380/55, 380/59
US-CL-CURRENT: 380/278; 380/281, 380/30, 380/51, 380/54, 380/55, 380/59, 713/158, 713/180

FIELD-OF-SEARCH: 380/9, 380/10, 380/20, 380/21, 380/23, 380/30, 380/49, 380/50, 380/51, 380/55, 380/59, 380/16, 380/54

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3736369	May 1973	Vogelman et al.	380/16
☐	3890461	June 1975	Vogelman et al.	380/16
☐	4081832	March 1978	Sherman	380/16
☐	4605846	August 1986	Duret et al.	
☐	5384846	January 1995	Berson et al.	380/23
☐	5420924	May 1995	Berson et al.	380/23

ART-UNIT: 362

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Reichman; Ronald Scolnick; Melvin J.

ABSTRACT:

This invention is a system for producing and distributing new decryption keys to verifiers. Verifier decryption key updates are printed in a secure manner on paper or postcards and mailed to the owners of the verifiers. The paper or postcards containing the verifier decryption key is scanned into the verifier and the verifier's key file is updated.

14 Claims, 4 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 16 of 20 File: USPT Sep 22, 1998

DOCUMENT-IDENTIFIER: US 5812664 A
TITLE: Key distribution system

Application Filing Date (1):
19960906

Detailed Description Text (10):
Computer 12 generates a unique client master cryptographic key pair, that includes an encryption key and a decryption key. Processor 18 of authenticator 13 generates a unique session cryptographic key pair, that includes an encryption key and a decryption key i.e. private and public key respectively The master cryptographic public-key is the key that unlocks the certificate. The certificate contains the session public key. The session public key is used to decrypt the session data. Session data may be the client public key, a certificate revocation, a new master public key or program updates for processor 37 of verifier 35. Authenticator 13 stores the private portion of session cryptographic key pair in memory 9 and transmits the public portion of session cryptographic key pair to computer 12.

Current US Original Classification (1):
380/278

L20: Entry 17 of 20 File: USPT Dec 17, 1996

US-PAT-NO: 5586186
DOCUMENT-IDENTIFIER: US 5586186 A

TITLE: Method and system for controlling unauthorized access to information distributed to users

DATE-ISSUED: December 17, 1996

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Yuval; Gideon A.	Mercer Island	WA		
Ernst; Michael	Redmond	WA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Microsoft Corporation	Redmond	WA			02

APPL-NO: 08/275500 [PALM]
DATE FILED: July 15, 1994

INT-CL: [06] H04 L 9/30

US-CL-ISSUED: 380/30; 380/4, 380/25
US-CL-CURRENT: 380/30; 380/45, 705/51

FIELD-OF-SEARCH: 380/4, 380/30, 380/25

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4405829	September 1983	Rivest et al.	380/30
☐	4658093	April 1987	Hellman	380/4
☐	4670857	June 1987	Rackman	380/4
☐	4944007	July 1990	Austin	
☐	5222133	June 1993	Chou et al.	380/4
☐	5319705	June 1994	Halter et al.	380/4

OTHER PUBLICATIONS

Desmedt, Yvo G. (ed.), Advances in Cryptology--Crypto '94, Proc. of the 14th Int'l Cryptology Conf., Santa Barbara, CA, Aug. 21-25, 1994, Springer-Verlag, Heidelberg, 1994, pp. 257-270.
Koyama et al., "New Public-Key Schemes Based on Elliptic Curves over the Ring Z.sub.n, "Advances in Cryptology--Crypto '91, Proc. of the 11th Int'l. Cryptology Conf., Springer-Verlag, Heidelberg, 1991, pp. 252-266.
Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Boston, MA, 1993, pp. 1-128.
Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21(2):120-126, 1978.
Cormen et al., Introduction to Algorithms, MIT Press and McGraw-Hill, pp. 801-852, 1990.
Hamming, "Error Detecting and Error Correcting Codes," The Bell System Technical Journal 26(2):147-160, 1950.
Tanenbaum, Computer Networks, 2d ed., pp. 206-212.
Blahut, Theory and Practice of Error Control Codes, pp. 54-55.
Vanstone et al., An Introduction to Error Correcting Codes with Applications, Kluwer Academic Publishers, pp. 65-69.
Encyclopedia of Mathematics and Its Applications, pp. 142-143.
Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., pp. 281-288, 1994.
Lewis et al., Elements of the Theory of Computation, Prentice-Hall, Inc., Engelwood Cliffs, NJ, pp. 242-248, 1981.
"The Arcade Project: A Progress Report," Ciphertext, The RSA Newsletter 2(1):6-7, 1994.
"Apple Computer: Launches Software Dispatch," Newswire Mailing, from Microsoft, Oct. 11, 1993, 136 lines.
Flynn, Mary Kathleen, "Software Samplers Coming on CD-ROM," PC Magazine, Sep. 28, 1993, 53 lines.

ART-UNIT: 222

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Seed and Berry LLP

ABSTRACT:

A system for controlling unauthorized access to information distributed to users and, more particularly, for controlling unauthorized access to software distributed to users is provided. One method utilizing the system of the present invention enables the software to be encrypted using a single encryption key and to be decrypted using a multiplicity of "decryption" keys, each of which is unique to a particular user. The "decryption" keys are the products of numeric representations of identifying information relating to users and unique user keys generated using the numeric representations and a "true" decryption key. Since each user receives a unique user key and both the numeric representation and the user key are generated using the identifying information, if the user reveals the numeric representation and the user key (or the product of the numeric representation and the user key), the numeric representation and the user key can be traced to the user who revealed them. Another method utilizing the system of the present invention introduces randomness or pseudo-randomness into the decryption scheme to provide an additional level of security to the scheme.

39 Claims, 10 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 17 of 20 File: USPT Dec 17, 1996

DOCUMENT-IDENTIFIER: US 5586186 A
TITLE: Method and system for controlling unauthorized access to information distributed to users

Application Filing Date (1):
19940715

Brief Summary Text (8):
Any solution involving encryption must be based on an encryption algorithm. Generally, there are two types of encryption algorithms, symmetric and public key. A symmetric algorithm is one in which the encryption key and the decryption key can be generated from each other. Often, the encryption key and the decryption key will be the same. A public key algorithm, on the other hand, is one in which the encryption key and the decryption key are different. Generally, the encryption key is made public, the decryption key is kept secret, and the private decryption key cannot be easily generated from the public encryption key.

Detailed Description Text (3):
The preferred embodiments of the present invention use a public key algorithm. As discussed above, a public key algorithm is one in which the encryption key and the decryption key are different. Generally, the encryption key is made public, the decryption key is kept secret, and the private decryption key cannot be easily generated from the public encryption key. More specifically, the preferred embodiments of the present invention use a modified RSA algorithm. The modified RSA algorithm used in the present invention is partially based on the RSA algorithm, but provides additional features not provided by the RSA algorithm (these additional features will be described in detail below).

Current US Cross Reference Classification (2):
705/51

CLAIMS:

20. A system for controlling unauthorized access to information distributed to users, the system comprising:

an encryptor for generating an encryption key and a decryption key using a public key algorithm and for encrypting the information using the encryption key;

a user key generator for receiving identifying information from a user, for generating a numeric representation of the identifying information, and for generating a unique user key using the numeric representation of the identifying information and decryption key information; and

a decryptor for decrypting the encrypted form of the information using the numeric representation of the identifying information and the unique user key.

L20: Entry 18 of 20 File: USPT Oct 27, 1992

US-PAT-NO: 5159633
DOCUMENT-IDENTIFIER: US 5159633 A
**** See image for Certificate of Correction ****

TITLE: Multimedia network system

DATE-ISSUED: October 27, 1992

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Nakamura; Kenji	Hadano			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Canon Kabushiki Kaisha	Tokyo			JP	03

APPL-NO: 07/641879 [PALM]
DATE FILED: January 15, 1991

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	2-008366	January 19, 1990

INT-CL: [05] H04L 9/30, H04N 7/167

US-CL-ISSUED: 380/30; 380/4, 380/5, 380/9, 380/10, 380/21, 380/43, 380/49
US-CL-CURRENT: 380/30; 380/200, 380/231, 380/282, 380/43, 705/51, 705/52, 713/180

FIELD-OF-SEARCH: 380/10, 380/20, 380/30, 380/49, 380/3-5, 380/9, 380/21, 380/43, 380/50, 380/46

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4245245	January 1981	Matsumoto et al.	
☐	4464678	August 1984	Schiff et al.	
☐	4623920	November 1986	Dufresne et al.	380/20

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
179612	April 1986	EP	
2161680	January 1986	GB	
8500718	February 1985	WO	
8806826	September 1988	WO	

OTHER PUBLICATIONS

BBC Research Department Report, Aug. 1988, Tadworth, Surrey, UK, pp. 1-18, D. T. Wright, "Conditional Access Broadcasting: Datacare 2, An Over-Air Enabled System For General Purpose Data Channels".

ART-UNIT: 222

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Fitzpatrick, Cella, Harper & Scinto

ABSTRACT:

There is disclosed a multimedia network system for transmitting real-time communication type information such as a television video signal and storage type information such as a computer file using at least one transmission path. The real-time communication type information is encrypted by a secret-key system, and the storage type information is encrypted by a public-key system. A common encryption key of the public-key system is changed in each communication. High-speed information can be safely encrypted and transmitted.

14 Claims, 10 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 18 of 20 File: USPT Oct 27, 1992

DOCUMENT-IDENTIFIER: US 5159633 A
**** See image for Certificate of Correction ****
TITLE: Multimedia network system

Application Filing Date (1):
19910115

Brief Summary Text (11):
In contrast to this, in the public-key cryptosystem, a pair of different encryption and decryption keys are used, and an encryption key is disclosed to all the terminals.

Brief Summary Text (26):
More specifically, a multimedia network system for transmitting real-time communication type information such as a television video signal and storage type information such as a computer file using at least one transmission path, comprises secret-key encryption means for encrypting the real-time communication type information by secret-key system in which only transmitting and receiving terminals of the information have encryption and decryption keys, public-key encryption means for encrypting the storage type information by a public-key system in which all the terminals commonly have their own encryption keys, and only a receiving terminal of the information has its own decryption key, and secret-key control means for causing the secret-key encryption means to change a common encryption key in each communication, and causing the public-key encryption means to encrypt and transmit the changed key.

Current US Cross Reference Classification (2):
380/231

Current US Cross Reference Classification (5):
705/51

CLAIMS:

1. A multimedia network system for transmitting real-time communication type information and storage type information using at least one transmission path, comprising:

a transmitting terminal comprising secret-key encryption means for encrypting the real-time communication type information by a secret-key system in which only transmitting and receiving terminals of the information have encryption and decryption keys, public-key encryption means for encrypting the storage type information by a public-key system in which all the terminals commonly share their own encryption keys, and only a receiving terminal of the information has its own decryption key, and control means for causing said secret-key encryption means to change a common encryption key in each communication, and causing said public-key encryption means to encrypt and transmit the changed key.

2. A multimedia network system for communicating real-time communication type information and storage type information using at least one transmission path,

comprising:

a receiving terminal comprising secret-key decryption means for decrypting the real-time communication type information by a secret-type system in which only transmitting and receiving terminals of the information have encryption and decryption keys, public-key decryption means for decrypting the storage type information by a public-key decryption means for decrypting the storage type information by a public-key system in which all the terminals commonly share their own encryption keys, and only a receiving terminal of the information has its own decryption key, and secret-key control means for causing said secret-key decryption means to change a common decryption key in each communication.

3. A multimedia network system for transmitting real-time communication type information and storage type information using at least one transmission path, comprising:

a transmitting terminal comprising secret-key encryption means for encrypting the real-time communication type information by a secret-key system in which only transmitting and receiving terminals of the information have encryption and decryption keys, public-key encryption means for encrypting the storage type information by a public-key system in which all the terminals commonly share their own encryption keys, and only a receiving terminal of the information has its own decryption key, and first control means for causing said secret-key encryption means to change a common encryption key in each communication, and causing said public key encryption means to encrypt and transmit the changed key; and

a receiving terminal comprising a secret-key decryption means for decrypting the real-time communication type information by secret-key system in which only transmitting and receiving terminals of the information have encryption and decryption keys, public-key decryption means for decrypting the storage type information by a public-key system in which all the terminals commonly have their own encryption keys, and only a receiving terminal of the information has its own description key, and second control means for causing said secret-key decryption means to change a common decryption key in each communication.

5. The system according to claim 3, wherein a file for ordering information from said receiving terminal to said transmitting terminal, and the real-time communication type information transmitted from said transmitting terminal to said receiving terminal in accordance with the file are encrypted using the secret-key by said secret-key encryption means, and a reception confirmation file for the real-time communication type information, which file is transmitted from said receiving terminal to said transmitting terminal, and a charge demand file from said transmitting terminal to said receiving terminal are encrypted by said public key encryption means, and are decrypted by the decryption key inherent to said receiving terminal.

Previous Doc Next Doc Go to Doc#

L20: Entry 19 of 20 File: USPT Feb 20, 1990

US-PAT-NO: 4903296
DOCUMENT-IDENTIFIER: US 4903296 A

TITLE: Implementing a shared higher level of privilege on personal computers for copy protection of software

DATE-ISSUED: February 20, 1990

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chandra; Akhileshwari N.	Mahopac	NY		
Comerford; Liam D.	Carmel	NY		
White; Steve R.	New York	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 06/930219 [PALM]
DATE FILED: November 12, 1986

PARENT-CASE:
This application is a division of U.S. Ser. No. 06/651,184 filed on Nov. 14, 1984, now U.S. Pat. No. 4,644,493.

INT-CL: [04] H04L 9/00

US-CL-ISSUED: 380/4; 364/969, 364/969.2, 364/969.4
US-CL-CURRENT: 705/56; 380/282, 705/57

FIELD-OF-SEARCH: 364/200, 364/900, 360/131, 380/3, 380/4, 380/49, 380/25

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4168396	September 1979	Best	364/900
☐	4246638	January 1981	Thomas	364/200
☐	4465901	August 1984	Best	364/200

☐	4558176	December 1985	Arnold et al.	364/900
☐	4573119	February 1986	Westheimer et al.	364/200
☐	4577289	March 1986	Comerford et al.	364/900

ART-UNIT: 237

PRIMARY-EXAMINER: Heckler; Thomas M.

ASSISTANT-EXAMINER: Mills; John G.

ATTY-AGENT-FIRM: Arnold; Jack M.

ABSTRACT:

Method and apparatus which restricts software, distributed on magnetic media, to use on a single computing machine. The original medium is functionally uncopyable, until it is modified by the execution of a program stored in a tamper proof co-processor which forms a part of the computing machine. The modified software on the original medium may then be copied, but the copy is operable only on the computing machine containing the co-processor that performed the modification.

4 Claims, 20 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 19 of 20 File: USPT Feb 20, 1990

DOCUMENT-IDENTIFIER: US 4903296 A
TITLE: Implementing a shared higher level of privilege on personal computers for copy protection of software

Application Filing Date (1):
19861112

Detailed Description Text (21):
3. The decryption key in encrypted form where the encryption is by the RSA public key provided by the support hardware manufacturer.

Current US Cross Reference Classification (2):
705/57

Refine Search

Search Results -

Terms	Documents
L1 and (encrypt$ same (decrypt$ with key$))	1

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L3

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Sunday, November 13, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L3	L1 and (encrypt$ same (decrypt$ with key$))	1	L3
L2	L1 and (encrypt$ same (decrypt$ with key$) same public$)	1	L2
L1	6072874.pn.	1	L1

END OF SEARCH HISTORY

L2: Entry 1 of 1 File: USPT Jun 6, 2000

DOCUMENT-IDENTIFIER: US 6072874 A
TITLE: Signing method and apparatus using the same

Brief Summary Text (6):
Japanese Patent Application Laid-Open No. Hei. 4-334227 (1992) discloses a method of forcing a user of charged broadcasting program to execute the digital signature on fee imposition information so that future denial of use of the charged program may be prevented. According to the invention of the Laid-Open publication, an encrypted program and a decryption key for decrypting the encrypted program are transmitted to a broadcasting program receiving decoder from the broadcasting station. The decoder receives the request for providing a program from the receiver, and notifies the receiver of the amount of the fee imposed on watching and listening to the program. If the amount of the fee is acceptable to the receiver, he/she executes digital signature with respect to the amount of the fee and returns it to the decoder. Then the decoder examines the returned digital signature of the amount of the fee to verify whether the signature is generated by a legitimate receiver. After legitimacy of the signature is verified, the decoder decrypts the requested program by the key obtained in advance, and provides the program to the receiver.

Detailed Description Text (9):
The secret key storing unit 32 stores a secret key D which makes a pair with the public key E. The decryption unit 33 decrypts key information K.sup.eE encrypted by the public keys E and e by utilizing the secret key D, and generates data K.sup.e. The concatenation computation unit 34 concatenates the data K.sup.e transmitted from the decryption unit 33 and a Hash value of the message by a predetermined computation and then transmits concatenated information to the authentication card 23. In the concatenated information, the encrypted key information k.sup.e is inseparable from the Hash value and they cannot be separated even if the key d stored in the authentication card 23 is used. In the authentication card 23, the computation is performed on the concatenated information by utilizing the key d, and the result of computation is provided to the separation computation unit 35.

L3: Entry 1 of 1 File: USPT Jun 6, 2000

DOCUMENT-IDENTIFIER: US 6072874 A
TITLE: Signing method and apparatus using the same

Abstract Text (1):
The present invention provides a signing apparatus used for signing by a user on usage information of a source provided in a format made available by the use of key information. The apparatus includes a unit for generating the usage information which is to be signed, a unit for performing a first computation by utilizing the key information which has been encrypted and the usage information, a unit for performing a second computation by utilizing a user's private key and a result of the first computation. The apparatus further includes a unit for performing a third computation by utilizing a result of the second computation, and thereby generating the key information which has been decrypted and a result of the computation performed on the usage information by utilizing the user's private key. The apparatus further includes a unit for making the source available by utilizing the decrypted key information.

Brief Summary Text (6):
Japanese Patent Application Laid-Open No. Hei. 4-334227 (1992) discloses a method of forcing a user of charged broadcasting program to execute the digital signature on fee imposition information so that future denial of use of the charged program may be prevented. According to the invention of the Laid-Open publication, an encrypted program and a decryption key for decrypting the encrypted program are transmitted to a broadcasting program receiving decoder from the broadcasting station. The decoder receives the request for providing a program from the receiver, and notifies the receiver of the amount of the fee imposed on watching and listening to the program. If the amount of the fee is acceptable to the receiver, he/she executes digital signature with respect to the amount of the fee and returns it to the decoder. Then the decoder examines the returned digital signature of the amount of the fee to verify whether the signature is generated by a legitimate receiver. After legitimacy of the signature is verified, the decoder decrypts the requested program by the key obtained in advance, and provides the program to the receiver.

Brief Summary Text (26):
Additional objects and advantages of the invention will be set forth in part in the description which follows and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims. To achieve the objects and in accordance with the purpose of the invention, as embodied and broadly described herein, the first aspect of a signing apparatus of the present invention used for executing signature by a user on usage information of a source provided in a format made to be available by the use of key information, comprises means for generating the usage information which is to be signed, means for performing a first computation by utilizing the key information which is encrypted and the usage information, means for performing a second computation by utilizing a user's private key and a result of the first computation, means for performing a

third computation by utilizing a result of the second computation, and thereby generating the key information which has been decrypted and a result of the computation performed on the usage information by utilizing the user's private key, and means for making the source available by utilizing the decrypted key information.

Brief Summary Text (28):
In the second aspect of the present invention, for a signing apparatus used for executing signature by a user on usage information of a source provided in a format made to be available by the use of key information; a guarding device which guards inside information from external access, means for generating the usage information which is to be signed, means disposed in the guarding device for performing a first computation by utilizing the key information which is encrypted and the usage information, means for performing a second computation by utilizing a user's private key and a result of the first computation, means disposed in the guarding device for performing a third computation by utilizing a result of the second computation, and thereby generating the decrypted key information and a result of the computation performed on the usage information by utilizing the key information of the user, and means disposed in the guarding device for making the source available by utilizing the decrypted key information are provided.

Brief Summary Text (31):
Moreover, in the second aspect, it may be possible to provide means for decrypting the information which has been encrypted by a key unavailable for the user in the guarding device so that the encrypted key information may be further encrypted by the key unavailable for the user, provided to the means for decrypting, and then the first computation may be performed on the key information decrypted by the means for decrypting.

Brief Summary Text (33):
Moreover, in the first and second aspects of the present invention, a plurality of encrypted key information may be generated for a single source and content of the usage information pared with key information may be a fact that the key information decrypted immediately before is used, and the use of the source may be closed when the user refuses to execute signature on the usage information.

Brief Summary Text (34):
In the third aspect of the present invention, for an information processing apparatus having a source providing system and a source using system; means disposed in the source providing system for protecting and then outputting a source, means disposed in the source providing system for encrypting and outputting key information for cancelling the protection, a guarding device disposed in the source using system for guarding inside information from external access, means disposed in the source using system for generating usage information which is to be signed, means disposed in the guarding device for performing a first computation by utilizing the encrypted key information and the usage information, means disposed in the source using system for performing a second computation by utilizing a private key of a user and a result of the first computation, means disposed in the guarding device for performing a third computation by utilizing a result of the second computation, and thereby generating the decrypted key information and a result of the computation performed on the usage information by utilizing the user's private key, and means disposed in the guarding device for making the source available by utilizing the key information are provided.

Brief Summary Text (36):
In the fourth aspect of the present invention, for a signing method used for signing by a user on usage information of a source provided in a format made to be available by the use of key information; steps of generating the usage information which is to be signed, performing a first computation by utilizing the encrypted key information and the usage information, performing a second computation

utilizing a result of the first computation and a user's private key, performing a third computation by utilizing a result of the second computation, and thereby generating the key information which has been decrypted and a result of the computation on the usage information by utilizing the user's private key, and making the source available by utilizing the key information are provided.

Brief Summary Text (38):
In the fifth aspect of the present invention, for a computer program product for use with a computer; a computer usable medium having computer readable program code means embodied in the medium for causing the computer to process signature executed by a user on usage information of a source provided in a format made to be available by the use of key information, computer readable program code means for causing the computer to generate usage information which is to be signed, computer readable program code means for causing the computer to perform a first computation by utilizing the key information which has been encrypted and the usage information, computer readable program code means for causing the computer to perform a second computation utilizing a result of the first computation and a private key of the user, computer readable program code means for causing the computer to perform a third computation by utilizing a result of the second computation, and thereby to generate the key information which has been decrypted and a result of the computation performed on the usage information by utilizing the private key of the user, and computer readable program code means for making the source available by utilizing the key information are provided.

Brief Summary Text (40):
In the sixth aspect of the present invention, for a signature verification apparatus used for executing signature by a user on usage information of a source provided in a format made to be available by the use of key information, means for generating the usage information which is to be signed, means for performing a first computation by utilizing the encrypted key information and the usage information to be signed, means for performing a third computation by utilizing a result of a second computation for decrypting the key information and signing performed on a result of the first computation by utilizing a user's private key, and thereby generating the key information which has been decrypted and a result of the computation performed on the usage information by utilizing the user's private key, and means for making the source available by utilizing the decrypted key information are provided.

Detailed Description Text (9):
The secret key storing unit 32 stores a secret key D which makes a pair with the public key E. The decryption unit 33 decrypts key information K.sup.eE encrypted by the public keys E and e by utilizing the secret key D, and generates data K.sup.e. The concatenation computation unit 34 concatenates the data K.sup.e transmitted from the decryption unit 33 and a Hash value of the message by a predetermined computation and then transmits concatenated information to the authentication card 23. In the concatenated information, the encrypted key information k.sup.e is inseparable from the Hash value and they cannot be separated even if the key d stored in the authentication card 23 is used. In the authentication card 23, the computation is performed on the concatenated information by utilizing the key d, and the result of computation is provided to the separation computation unit 35.

Detailed Description Text (12):
On the other hand, the encrypted key information K.sup.eE is received by the decryption unit 33 and decrypted into the data K.sup.e by utilizing the key D (steps 110 and 111). The concatenation computation is executed on the data K.sup.e and the Hash value. The concatenated information generated by the concatenation computation is provided to the authentication card 23 (steps 112-114). The authentication card 23 receives the concatenated information, and in the Hash value checking unit 29, the message is checked by utilizing the Hash value (steps 106 and 107). After the check is completed, the signature computation unit 30 performs the

signature computation by using the secret key d (step 108), and the result of computation is provided to the separation computation unit 35 of the signature information issuing unit 21 (step 115).

CLAIMS:

1. A signing apparatus used for signing by a user on usage information of a source provided in a format made to be available by the use of key information, comprising:

means for generating said usage information which is to be signed;

means for performing a first computation by utilizing said key information which has been encrypted and said usage information;

means for performing a second computation by utilizing a private key of said user and a result of said first computation;

means for performing a third computation by utilizing a result of said second computation, and thereby generating said key information which has been decrypted and a result of said computation performed on said usage information by utilizing said private key of said user; and

means for making said source available by utilizing said decrypted key information, wherein said means for performing the first computation assumes the product of two large prime numbers to be a modulus, the two large prime numbers not being known to said user and, using said modulus, generates a first diagonal matrix having said encrypted key information and said usage information as components, and produces a second matrix from said first matrix, said second matrix being a different representation of said first matrix using an arbitrary basis.

2. A signing apparatus used for signing by a user on usage information of a source provided in a format made to be available by the use of key information, comprising:

a guarding device for guarding inside information from external access;

means for generating said usage information which is to be signed;

means disposed in said guarding device for performing a first computation by utilizing said key information which has been encrypted and said usage information;

means for performing a second computation by utilizing a private key of said user and a result of said first computation;

means disposed in said guarding device for performing a third computation by utilizing a result of said second computation, and thereby generating said key information which has been decrypted and a result of said computation performed on said usage information by utilizing said private key of said user; and

means disposed in said guarding device for making said source available by utilizing said decrypted key information, wherein said means for performing the first computation assumes the product of two large prime numbers to be a modulus, the two large prime numbers not being known to said user and, using said modulus, generates a first diagonal matrix having said encrypted key information and said usage information as components, and produces a second matrix from said first matrix, said second matrix being a different representation of said first matrix using an arbitrary basis.

4. The signing apparatus according to claim 2, further comprising:

means disposed in said guarding device for decrypting information which has been encrypted by a key unavailable for said user, wherein said encrypted key information is further encrypted by said key unavailable for the user and provided to said means for decrypting, and said first computation is performed on said key information decrypted by said means for decrypting.

9. A signature verification apparatus used for signing by a user on usage information of a source provided in a format made to be available by the use of key information, comprising:

means for generating said usage information which is to be signed;

means for performing a first computation by utilizing said key information which is encrypted and said usage information which is to be signed;

means for performing a third computation by utilizing a result of a second computation for decrypting key information and signing performed on a result of said first computation by utilizing a private key of said user, and thereby generating said key information which is decrypted and a result of said computation performed on said usage information by utilizing said private key of said user; and

means for making said source available by utilizing said decrypted key information, wherein said means for performing the first computation assumes the product of two large prime numbers to be a modulus, the two large prime numbers not being known to said user and, using said modulus, generates a first diagonal matrix having said encrypted key information and said usage information as components, and produces a second matrix from said first matrix, said second matrix being a different representation of said first matrix using an arbitrary basis.

13. A signing apparatus used for signing by a user on usage information which shows using a source provided in a format made to be available by the use of key information, comprising:

means for inputting said key information encrypted by a key which makes a pair with a private key of said user;

means for storing said private key of said user;

means for generating usage information which is to be signed;

means for concatenating said encrypted key information, inputted by said means for inputting said key information, and said usage information generated by said means for generating usage information;

signing means for executing decryption of said encrypted key information of said concatenated information by utilizing said private key of said user stored in said means for storing, and for signing said usage information generated by said means for generating said usage information of said concatenated information by utilizing said private key of said user stored in said means for storing;

means for separating said information processed by said signing means into said decrypted key information and said usage information which has been signed; and

means for making said source available by utilizing said decrypted key information separated by said means for separating, wherein said means for concatenating assumes the product of two large prime numbers to be a modulus, the two large prime numbers not being known to said user and, using said modulus, generates a first

diagonal matrix having said encrypted key information and said usage information as components, and produces a second matrix from said first matrix, said second matrix being a different representation of said first matrix using an arbitrary basis.

Previous Doc Next Doc Go to Doc#

L20: Entry 1 of 20 File: USPT Jun 21, 2005

US-PAT-NO: 6910020
DOCUMENT-IDENTIFIER: US 6910020 B2

TITLE: Apparatus and method for granting access to network-based services based upon existing bank account information

DATE-ISSUED: June 21, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Oyama; Shuji	Kawasaki			JP
Sato; Akira	Kawasaki			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Fujitsu Limited	Kawasaki			JP	03

APPL-NO: 08/825565 [PALM]
DATE FILED: March 31, 1997

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	08-273153	October 16, 1996

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/38; 705/50, 705/71, 705/76, 380/232, 380/228, 713/200, 713/201
US-CL-CURRENT: 705/38; 380/228, 380/232, 705/50, 705/71, 705/76, 726/10

FIELD-OF-SEARCH: 705/35, 705/38, 705/42, 705/44, 705/64, 705/74, 705/76, 705/39, 705/70, 705/71, 235/379, 235/380, 380/24, 380/25, 380/49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5193057	March 1993	Longfield	
☐	5606496	February 1997	D'Agostino	
☐	5703949	December 1997	Rosen	

☐	5765144	June 1998	Larche et al.	
☐	5790665	August 1998	Micali	
☐	5797133	August 1998	Jones et al.	
☐	5859419	January 1999	Wynn	
☐	5866889	February 1999	Weiss et al.	
☐	5870721	February 1999	Norris	
☐	5878403	March 1999	DeFrancesco et al.	
☐	5911135	June 1999	Atkins	
☐	6354490	March 2002	Weiss et al.	235/379
☐	2001/0002468	May 2001	Nel	705/26

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
02-287767	November 1990	JP	
402287767	November 1990	JP	
08-235277	September 1996	JP	

OTHER PUBLICATIONS

"Community Group Keeps Watchful Eye on Goldome", American Banker, p. 6, Feb. 26, 1990.
Thoren-Paden et al., "Compliance Issues in Cyberspace", ABA Bank Compliance, V17N5, pp12-22, May 1996.
"How Institutions Can Prepare for "Know Your Customer" Regs", Money Laundering Alert, V5N4, Jan. 1994.
"SCAN OnLine Defines New Era in the Fight Against Check Fraud", PR Newswire, Sep. 1996.
"Fed's Examiners Get Roadmap to KYC Weaknesses in Banks", Money Laundering Alert, vol. 6, No. 7, Apr. 1995.
"Banks Run Risk of BSA, OFAC Dangers in Cyberbanking", Money Laundering Alert, Oct. 1, 1996.
English-language translation of relevant parts of Japanese Laid-open No. 2-287767 (Makoto), 1 page.

ART-UNIT: 3621

PRIMARY-EXAMINER: Backer; Firmin

ATTY-AGENT-FIRM: Staas & Halsey LLP

ABSTRACT:

A network transaction system applicable to cyberspace banking services using an open network, which allows customers to authenticate themselves through a simplified procedure. A customer's terminal station and a plurality of bank systems are interconnected via networks, and it is assumed that the customer wishes to newly open a bank account in a bank system among them, or a target bank system, and that the customer has an existing bank account in a different bank system, or an

cooperative bank system. Using his/her terminal station, the customer applies for a new bank account by supplying the target bank system with a ciphertext message containing existing account information descriptive of the customer's bank account in the cooperative bank system. The target bank system requests the cooperative bank system to confirm the customer's existing bank account, while forwarding thereto a part of the ciphertext message containing the existing account information. The cooperative bank system decrypts the received message and confirms the validity of the account that the customer claims to own. It then returns a response message to the target bank system to report the result of the account confirmation. The target bank system decides whether to accept or to reject the application for a new account based on the response message from the cooperative bank system.

6 Claims, 7 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 1 of 20 File: USPT Jun 21, 2005

DOCUMENT-IDENTIFIER: US 6910020 B2
TITLE: Apparatus and method for granting access to network-based services based upon existing bank account information

Application Filing Date (1):
19970331

Detailed Description Text (32):
FIG. 4 depicts a flow of encrypted information, where the RSA public-key encryption algorithm is widely adopted. In general, public-key cryptosystems use a pair of encryption/decryption keys, namely, a secret key and a public key. One of those keys is used to encrypt messages, which can be decrypted only by using the other key. For example, FIG. 4 shows that a customer secret key px and a customer public key ox are assigned to a customer X (i.e., the terminal station 10). Similarly, a target bank secret key py and a target bank public key oy are assigned to a target bank Y (i.e., the target bank system 30), while a cooperative bank secret key pz and a cooperative bank public key oz are assigned to a cooperative bank Z (i.e., the cooperative bank system 50).

Current US Cross Reference Classification (2):
380/232

L20: Entry 2 of 20 File: USPT Mar 4, 2003

US-PAT-NO: 6530020
DOCUMENT-IDENTIFIER: US 6530020 B1
**** See image for Certificate of Correction ****

TITLE: Group oriented public key encryption and key management system

DATE-ISSUED: March 4, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Aoki; Ryuichi	Kanagawa			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Fuji Xerox Co., Ltd.	Tokyo			JP	03

APPL-NO: 09/099308 [PALM]
DATE FILED: June 18, 1998

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-164506	June 20, 1997

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 713/163; 380/278, 380/279, 380/282, 380/284
US-CL-CURRENT: 713/163; 380/278, 380/279, 380/282, 380/284

FIELD-OF-SEARCH: 713/163, 380/278, 380/279, 380/282, 380/284

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4200770	April 1980	Hellman et al.	
☐	5748736	May 1998	Mittra	713/163
☐	5953419	September 1999	Lohstroh et al.	713/165

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
7-297818	April 1994	JP	

ART-UNIT: 2131

PRIMARY-EXAMINER: Hayes; Gail

ASSISTANT-EXAMINER: Seal; James

ABSTRACT:

In a public key encryption system where an individual is used as a unit, an idea of "group" is newly introduced. Then, both an encryption process operation of a plain text by an arbitrary member belonging to the group, and a decryption process operation of cryptogram information can be executed by employing such a combination key made from a group public key and a group secret key, which are produced in unit of "group", and further an individual public key and an individual secret key. With employment of this encryption system, while high secrecies can be maintained inside and outside the group, the cryptogram information can be commonly shared based upon a confirmation of a member among members within the group. Also, an electronic signature can be made by a member belonging to the group.

23 Claims, 17 Drawing figures

Previous Doc Next Doc Go to Doc#

L20: Entry 2 of 20 File: USPT Mar 4, 2003

DOCUMENT-IDENTIFIER: US 6530020 B1
**** See image for Certificate of Correction ****
TITLE: Group oriented public key encryption and key management system

Application Filing Date (1):
19980618

Brief Summary Text (16):
Further, the present invention provides a decryption apparatus used in a public key encryption system arranged by a combination between a first key P and a second key S, the first key P being used in a data conversion for encrypting a plain text, and the second key S being different from the first key P and being used in a data conversion for decrypting a cryptogram to produce a plain text, comprising secret key decrypting means for decrypting an encrypted secret key Pj(S) based upon an own secret key Sj, or a secret key of a group, the encrypted secret key Pj(S) being produced by encrypting a decryption key S used to decrypt a cryptogram sentence based upon a public key Pj of a receiver of a cryptogram; and decrypting means for decrypting the cryptogram sentence based upon a decryption key S which is decrypted by the secret key decrypting means to be acquired.

Current US Cross Reference Classification (1):
380/278

CLAIMS:

2. The computer readable recording medium as claimed in claim 1, wherein said encrypted cryptogram information is a decryption key S1 of another cryptogram information, and said encrypted group secret keys P.sub.Mi (S.sub.G) are decrypted by the member secret key S.sub.Mi specific to each of said members Mi to thereby acquire said group secret key S.sub.G, P.sub.G (S1) equal to said decryption key S1 which is encrypted by said group public key P.sub.G is decrypted by said group secret key S.sub.G to thereby acquire said decryption key S1, and said another cryptogram information is decrypted by said acquired decryption key S1.